



***Consultation Paper on “Review of the Telecom Commercial Communications Customer Preference Regulations, 2018”***

*Comments by Tata Teleservices Limited & Tata Teleservices (Maharashtra) Limited.*

At the outset, Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited [together called “TTL”] express our sincere gratitude to Telecom Regulatory Authority of India (TRAI) for releasing Consultation Paper on “*Review of the Telecom Commercial Communications Customer Preference Regulations, 2018*” and giving an opportunity to share our response.

In this respect we, TTL, would like to submit its response to the issues and concerns as mentioned in the Consultation Paper are follows:

1. TRAI has issued the *Telecom Commercial Communications Customer Preference Regulations, 2018*, on July 19th, 2018, through which it has mandated telecom licensees to implement Blockchain based Distributed ledger Technology (DLT) based systems and processes to control spam and It is noteworthy that this is one of the largest use cases of Blockchain and DLT in telecom, globally
2. Being designed with a co-regulatory approach, industry deliberated and designed each solution and process through mutual coordination and consensus and remained committed to the objective of curbing the menace of Unsolicited Commercial Communication (UCC).
3. The Telecom Service Providers (TSPs) have already implemented given modules:
  - a. Consumer Preference Registration Module
  - b. Entity/Registered Tele Marketer and Header Registration Module
  - c. Complaint Management Module
  - d. Scrubbing based on Principal Entity-ID and Header
  - e. Blocking traffic from unregistered headers



- f. Content Template Registration
  - g. Content Template Scrubbing
  - h. Digital Consent Acquisition
  - i. Registration of Consent Template
  - j. Scrubbing of the Service Explicit messages
  - k. Whitelisting of URLs
  - l. Implementation of Voice Solution 140 Series
  - m. Quarterly header and template verification
  - n. Preference and consent scrubbing
4. The ecosystem as prescribed by TRAI vide TCCCP 2018 requires the participation of various constitutional bodies, government organizations, principal entities, telemarketers etc. i.e. the complete implementation of the regulation is not in the hands of TSP alone. The number of stakeholders involved in implementing the Regulation is humongous and adequate time was required to bring all these stakeholders together with a common approach, understanding of the Regulation and implementation requirements.
5. The implementation of this regulation required awareness and involvement of all stakeholders in ecosystem (e.g. Government Organizations, Banks, Commercial Organisations, other Principal Entities, Telemarketer, Aggregators, TSPs, Consumers etc.). Implementation of this novel solution took time due to various complexities resulting from its massive scale and sheer number of stakeholders involved.
6. The Telecom industry, while making all efforts including spreading awareness and addressing most complex has crossed many milestones and the progress of regulations was closely reviewed by TRAI, regularly, by way of review meetings
7. Considering the above factors, we submit that TRAI should take into account the development process required to implement various modules prescribed by the Authority. TRAI may also consider the various challenges faced by the industry before making any changes to the DLT Platform.
8. Further the primary and specific focus of the TCCCP Regulation, 2018, is to mitigate UCC.



The scope of the TCCCP Regulation is focussed on protecting consumers from unsolicited marketing messages and ensuring that telecom operators implement robust mechanisms to prevent such communication.

9. Therefore, the TCCCP Regulation, 2018, focuses on curbing unsolicited communications and ensuring a transparent, consumer-friendly telecom environment. While fraud prevention is important, telecom service providers (TSPs) have limited role in prevention of the same. Instead, those engaging in fraud, such as phishing and scamming, should be held accountable and punished under the law to safeguard consumers and maintain trust in the telecom networks.
10. We request the Authority to consider that while the adoption of DLT is poised to enhance the transparency and security in managing unsolicited commercial communications (UCC), the financial and operational impact on TSPs and associated stakeholders should also be a key consideration.

The costs of technological upgrades, training, and onboarding processes are likely to be substantial. Thus, TRAI's regulatory approach will need to balance these costs against the expected benefits, such as improved data integrity, customer protection, and long-term operational efficiencies across the telecom sector.

**Question 1: Stakeholders are requested to submit their comments in respect of definitions of messages and calls and their categorizations, as suggested in the paragraphs 2.14 to 2.19 along with necessary justifications**

1. Transactional Messages and Calls:

- Definition: Transactional messages and calls should be defined as communications sent by a sender to its own customer/subscriber in response to a customer-initiated transaction or due to an existing long-term relationship. Examples include OTPs, e-commerce order tracking, Order delivery, transaction confirmations, balance alerts, travel reminders, rescheduling notifications, refund information, product/warranty information, renewal reminder, doctor appointment confirmation and follow up.



**For voice calls, validated OTP shall be considered as consent which should be flowing to DLT/third party consent gateway with option of revocation (Opt-out).**

- Few scenarios of service and transactional scenarios
  - Welcome call, KYC Related Communication
  - Bank Transactions - Cheque, Foreign Remittance, Suspected Fraud, OTPs
  - Product/Food Delivery/Goods Delivery/Cab Booking related communication
  - New Insurance Confirmation, Renewal Reminders
  - Payment Reminders, Confirmation, Collection
  - Doctors, Diagnostics appointment and confirmation
  - Appointment confirmation for Counselling and admission, Fee Reminders.
  - Ticket booking, Lab reports.
- Justification: This definition aligns with global best practices, such as those in the USA under the Telephone Consumer Protection Act (TCPA), which clearly distinguishes transactional communications from promotional ones. This clarity helps in preventing misuse and ensures that customers receive essential information without unnecessary interruptions.

## 2. Promotional Messages and Calls:

1. Definition: Promotional messages and calls should be defined as commercial communications containing promotional material or advertisements of a product or service. These communications should only be sent to customers who have not opted out such communications through DND/preference registration or have given explicit digital consent. Example of such content is like calling for new product offerings, up sell a new product etc.
  - Scenarios where a customer proactively reaching out to principal entity for exploring product and services offered by them and gives consent. PEs should give option to revoke consent to such customers at any time if they don't want further follow-up calls.



- Such scenarios may be categorized under service as PE is responding basis request initiated by customer.

## 2. Government Messages and Calls:

- **Definition:** Government messages and calls should be defined as communications transmitted on the directions of the Central Government, State Government, or bodies established under the Constitution, or by an agency expressly authorized by the Authority.
- **Justification:** These communications are in the public interest and should not require explicit consent. This categorization ensures that important information from government bodies reaches the public without unnecessary barriers. For example, communication sent to masses for awareness programs, disaster management related communication, Covid related advisories etc. These messages/calls should not require consent and should be allowed without any blocking.
- Election campaign calls need to be clearly defined for its category to TSP.

**Question 2: Whether explicit Consent be made mandatory for receiving Promotional Communications by Auto Dialer or Robo Calls? What can be other possible measures to curb the use of Auto Dialer or Robo Calls without the consent of the recipients? Stakeholders are requested to submit their suggestions quoting best practices being followed across the world**

**TTL Response:** We recommend maintaining the current process and not implementing any changes to the requirement for explicit consent to receive promotional communications via auto-dialers or robo calls.

However, we recommend that PEs be actively onboarded to utilize the DCA process considering following inputs:

1. One-time bulk consent upload on DTL option to be given (directly or thru Third-party agency appointed for consent) with defined 1 year validity. Revocation option with customer at any time.



2. Third party Consent Gateway for capturing customer consent through API integration – Customer either puts OTP and confirms consent or scans the QR and agrees to terms of consent.
3. Zero Cost of consent acquisition is to be mandated.
4. Option for revocation of consent to be given to customer/PE/TSP.

**Question 3: As most of the pre-recorded calls have pre-defined content, stakeholders are requested to comment on the process to be followed to scrub such content before the delivery to consumers. The comments should be supported with suitable justifications and practices being followed in other parts of the world.**

**TTL Response:** We would like to submit that existing provisions of TCCCPR 2018 regulation already have significant measures to regulate unsolicited commercial communications, such as mandatory scrubbing of customer preferences against a Do Not Disturb (DND) registry and consent mechanisms

Under the TCCCPR 2018 framework, TSPs already follow rigorous scrubbing processes to filter out communications to consumers who have registered on the DND list or who have opted out of receiving certain types of communications. This scrubbing process is carried out through the Distributed Ledger Technology (DLT) platform, where content templates and headers are registered, and communication is only allowed if it complies with pre-approved templates.

Thus, the TCCCPR, 2018 regulations have already laid a solid foundation for controlling unwanted communications by ensuring that only authorized and pre-registered content is delivered. As far as Digital consent Acquisition (DCA) is concerned, we need to have additional mechanism to acquire DCA. Following can be the options

1. One-time bulk consent upload on DTL option to be given (directly or thru Third-party agency appointed for consent) with defined 1 year validity. Revocation option with customer at any time.
2. Third party Consent Gateway for capturing customer consent through API integration – Customer either puts OTP and confirms consent or scans the QR and agrees to terms of consent.



3. Zero Cost of consent acquisition is to be mandated.
4. Option for revocation of consent to be given to customer/PE/TSP

**Question 4: Stakeholders are required to submit their comments in respect of Headers identifiers categories as suggested in paragraphs 2.31 of Chapter-II or any other type of identifiers which may facilitate consumers to identify senders distinctly. Suggestions if any, should be suitably brought out with necessary justifications.**

**TTL Response:** We are of the opinion that the header identifiers which have already been discussed and tested by the industry is sufficient. We recommend maintaining the current process as of now.

**Question.5: Whether current provisions in the regulations for redressal of consumers' complaints in a time-bound manner are sufficient? If not, what provisions should be made for improving the effectiveness of the complaint handling processes including identifying and fixing the responsibilities of the violators?**

**TTL Response:** Regulation 25 of TCCCPR 2018 assign a significant role to Access Providers in handling consumer complaints, there is a growing need to fix clearer responsibilities and accountability on PEs, TMs and VNOs. The onus should primarily lie on these entities, as they are the originators of commercial communications, whether promotional or transactional. By making PEs and TMs directly accountable for UCC violations, the process of redressal can become more efficient and enforceable. To strengthen the complaint handling process, specific penalties and obligations must be imposed on PEs and TMs for recurring violations. Rather than placing the entire burden of complaint resolution on Access Providers.

Further the first level due diligence must be carried out at TAP level to be continued before forwarding the complaints to OAP. As far as timelines are proposed few SLAs cannot be met considering the various practical reasons like 2 hours SLA to get the CDRs from backend systems, weekends, public holidays etc. to be excluded. Business days to be considered with the timelines given in the TCCCPR-2018 regulations.



Current complaints handling involves validation of CDRs, checking with PE (in absence of digital consent, response time in co-ordination) or TAP. For enterprise customers, this process is even more complex due to high number of calls. For the same reasons, no. of calls after which outgoing restriction is proposed also need to be looked at. Enterprise calls should be handled with number of instances and not on number of complaints. It takes lot of time in closing the complaints. DCA with easy methodology will save lot of time in handling and closing complaints. Additional methods of DCA are already mentioned above (reproducing again)

1. One-time bulk consent upload on DTL option to be given (directly or thru Third-party agency appointed for consent) with defined 1 year validity. Revocation option with customer at any time.
2. Third party Consent Gateway for capturing customer consent through API integration – Customer either puts OTP and confirms consent or scans the QR and agrees to terms of consent.
3. Zero Cost of consent acquisition is to be mandated.
4. Option for revocation of consent to customer/PE/TSP

It is further to be noted that a clear definition of responsibilities among PEs, TMs, VNOs and TSPs will not only improve compliance but also ensure that consumers' rights are protected effectively

It would be helpful to establish more specific and realistic timelines that reflect the nature of the complaint (Like delay in getting response from PE) and the resources needed for resolution, particularly for enterprise customers. Additionally, the regulations currently do not specify the specific process including complaints handling for Enterprise Customers.

The current complaint resolution framework could be improved by defining financial securities with mandatory Security Deposit from PE/TM to Originating Access Provider a minimum amount of rupees one lakh only (Rs. 1,00,000/-) as refundable security deposit which may be specified in the agreement and Originating Access Provider shall be entitled to deduct from such security deposit based on complaint count by violating PE/TM from any registered or unregistered resources and additional security deposit may be charged.





Also, fixing key accountability on these entities and imposing stricter penalties for violations. This will not only enhance compliance but also ensure a smoother and more efficient complaint resolution process. Strengthening the role of PEs and TMs, alongside better collaboration with Access Providers, can address gaps in the current system, thereby offering better protection to consumers from unwanted communications.

Important to make the digital consent process opting in very easy for the customer and also free of cost.

This will ensure all complaints against calls without digital consent are acted upon on a timely basis without getting into too investigation and hence delays etc.

**Question.6: Whether facilities extended by the Service providers through Apps, Website and Call Centres for handling UCC complaints are accessible and consumer-friendly? Is there a need to add more facilities in the current systems? What measures should be taken by the service providers to make their Apps, Website and Call Centers easily accessible to the Consumers for registering UCC Complaints and tracking the same for a time-bound disposal of complaints? Please provide your answer with full details on the facilities needed.**

**TTL Response:** Current facilities are enough but mobile application can be added with voice mail feature for recording of the call and used as a proof of the call for lodging a complaint to be identified as SPAM/Fraud.

Service providers should keep on evolving/add more features to their system/apps to bring more accessibility to their customers.

However, the responsibility for ensuring that facilities provided for handling UCC complaints through apps, websites, and call centers are accessible and user-friendly should largely be left to the discretion of the TSPs. It is to be noted that the TSPs possess the technical expertise, customer insights, and operational understanding necessary to determine the best practices suited for their unique customer bases.



Therefore, we recommend that these initiatives should be left to TSPs, giving them the flexibility to innovate and deliver the best solutions for their customers. By doing so, TSPs can ensure that their systems are not only compliant but also efficient and consumer-friendly, leading to better management of UCC complaints in a manner that suits both the company and its users.

Additional provisions can be made to integrate such platform(app/website/social media) with Third party consent gateway and/or DLT.

**Question.7: What additional modes of complaints registration, preference registration and consents registration through a very easy and quick process can be implemented? Distributed Ledger(s) for Complaints (DL-Complaints).**

**TTL Response:** We do not recommend any changes to the existing complaint mechanism and suggest that the current framework should be maintained, along with ongoing awareness programs to support its effectiveness.

- May be social media channels can also be extended for such complaints, where TSP can defined mandatory inputs to be filled by customers.
- Validity of the consent should be valid till customer revoke/opt-out from the consent given.

**Question.8: Stakeholders are required to submit their comments on the following-**

- a. **Measures required for pro-active detection of spam messages and calls through honeypots and norms for the deployment of Honeypots in a LSA, and rules or logics required for effective use of AI-based UCC detection systems including training of AI models for identification, detection and prevention of spam**
- b. **Proactive actions needed to stop further communications of messages or calls identified as spam through UCC detect systems and actions on the senders.**

**TTL Response:** Proactive detection of spam messages and calls can be enhanced by:

- Deploying honeypots can be effective in case of auto dialer/robo calls/bulk calling terminating on mobile numbers. At the same time current honey pots which have been deployed in enterprise have not supported much as there are hardly any calls



on wireline number. It is further to mention that wireline operators are not present in all SDCAs of a circle and have centralized operations of call centres/IVR recording. **In view of this it is suggested that honeypot deployment should not be applicable in case of wireline enterprise operators.**

- Data analytics or automation tool analyse patterns of calling and complaints data.
- Implementing real-time feedback mechanisms to verify/validate suspected spam like call recording using mobile phone or app and using it as proof of detect along with CDR, date, time of the call and no of complaints.

**Question.9 Stakeholders are required to submit their comments in respect of**

- a. Financial disincentive proposed in the descriptions above on the access providers against violations in respect of RTMs**
- b. Financial disincentive proposed in the descriptions above on the access providers against violations in respect of UTMs**
- c. Financial disincentive proposed against wrong approval of Headers and Message Templates as per descriptions above on the access providers.**
- d. Measures needed to assign the responsibilities of telemarketers (both RTMs and UTMs) and Principal Entities (Senders), involved in sending UCC and disincentivize them financially including legal actions as per law**

**TTL Response:** The DLT system deployed by each TSP is capturing the details of each telemarketer as per current feasibility. In case such provisions are not able to stop the spam/fraud which is being managed with the different logics of capturing the data shared by entities. In this case also TSP are held liable while TSPs are carrying out due diligence while onboarding of the customer. It is the joint responsibility of the TSP, entity and aggregator.

In the current scenario, entities have no option but to use UTM for making service or transactional calling. If there are misuse of such resource, actions are taken which includes disconnection and blacklisting. At the same time there is genuine need of commercially use 160XX allocated for BFSI and govt. entity.



Another area of concern with the entities is related to SPAM tagging with 140XX series. There are entities/application providers/handset manufacturers in the market which misuse their wider reach with end customer. Such Application service providers are monetizing resources without owning anything and genuine numbers are also tagged as SPAM. This has already been raised as a problem and need to be addressed to bring these entities under regulatory regime. There are individual customers and Enterprise customers therefore such huge penalties to TSP are not justified. It is PE/TM/individual who should be penalized.

Additionally, there are cases where VNO and aggregators also onboard end customers which are not visible to TSP and not visible on DLT. Such use cases need to be regulated, and such entities also come under ambit of TRAI TCCCPR regulations.

Similarly, there is no check and control on OTT players providing similar services of voice and SMS and not bound by any such regulation. They also need to be made part of TCCCPR regulation to make effective implementation of SPAM/fraud control.

There are no fixed and definite guidelines for header approvals, and they are approved on a best effort basis by Header registrar. Financial disincentive proposed against wrong approval of headers need to be strengthened with well-defined criteria and continuous improvement.

We propose charging mechanism for content templates so that Principal Entities create only limited templates and avoid multiple templates which can lead to UCC/Fraud.

We are of the view that Financial Disincentives do not serve the purpose. We believe that the intention of TRAI is to reduce the menace of UCC from the financial disincentive. We are of the view that operators have made all the efforts that have considerably reduced their UCC complaints to a very low level and hence should not be penalized for unwarranted actions of some subscribers.

Thus, we suggest that financial disincentives be designed to effectively reduce unsolicited commercial communications (UCC) rather than imposing penalties exclusively on Access



Providers. A more balanced approach would ensure that the focus is on mitigating UCC issues rather than merely penalizing.

It is also important to clearly define the responsibilities of telemarketers and Principal Entities (Senders) to ensure accountability. Financial disincentives and legal actions should be used judiciously to encourage compliance. However, the focus should be on establishing effective compliance mechanisms with improvements in process rather than relying on financial penalties.

**Question.10: Whether there is a need to review five paisa exemptions accorded to transactional messages and bring them at par with other commercial messages? If yes, please give your answer with necessary justifications? If no, what additional measures are required to discourage senders, telemarketers or service providers from using transactional message templates for sending promotional messages?**

**TTL Response:** We are of the view that there is no need to review the exemptions accorded to transactional messages.

**Question.11 Stakeholders are requested to offer their comments on the following issues:**

**a. Whether there is a need to strengthen the provisions of Common Code of Practice templates with Standard Operating Processes further to enable Access Providers to take actions including imposing financial disincentives and actions as per law, against entities registered and not following the regulations? If so, what could be additional provisions and essential processes which should be made part of CoPs?**

**b. Whether there should be provision for minimum security deposits from the entities registering with any of the Access Providers, against the misuse or breach of regulations? If so, what should be the provisions in the CoPs for full or partial encashment/replenishment of security deposits against the breach of the regulations? Please provide your answers with suitable justifications.**

**TTL Response:** The provisions of the Common Code of Practice should be strengthened to enable access providers to take effective actions against non-compliant entities. This can include:



**TRAI should define clear processes and regulations specifically targeting senders who fail to comply with regulations.**

**Providing clear guidelines for imposing financial disincentives to entities/individuals**

**VNO, Aggregators and OTT players should be part of the overall TCCCPR ecosystem and COP.**

Currently there is no parity w.r.to the processes being followed by all TSPs, which is seen as loophole by violators. A standard framework needs to be defied under guidance of TRAI and followed by all TSP. this also needs to have a good governance model to ensure that the laid down process is being followed in similar ways across.

A robust legal framework is necessary to enforce penalties, including financial disincentives, against non-compliant entities. This will ensure that Access Providers have the necessary tools to take appropriate action. Additionally, **it is crucial to establish well-defined responsibilities for senders and to make senders directly accountable by registering them with TRAI. This approach would facilitate more effective enforcement of regulations and penalties.**

CoPs should clearly outline the **conditions under which security deposits can be fully or partially encashed or replenished. This includes specifying the procedures for claiming deposits in case of breaches and the process for replenishing them. Proper legal backing is needed to enforce these requirements and to ensure that security deposits serve their intended purpose.**

Aligning regulations and penalties equally for senders and principal entities, and establishing clear responsibilities, will help create a more comprehensive and effective regulatory environment

**Question 12: What effective steps can be taken to control the menace of UCC through tariffs? Please justify your answer.**

**TTL Response:** No Comments



**Question 13: Whether differential tariff for SMS and Voice calls beyond a certain limit should be introduced to disincentivize UCC through UTMs? Please justify.**

**TTL Response:** No Comments.

**Question 14: If differential tariff is introduced, what could be the limit beyond which differential tariff could be introduced for:**

- i. Voice Calls**
- ii. SMS.**

**Please justify with rationale.**

**TTL Response:** No Comments.

**Question 15: If differential tariff is introduced, what could be the tariff beyond a limit for:**

- i. Voice calls.**
- ii. SMS.**

**Please justify with rationale.**

**TTL Response:** No Comments.

**Question 16: Whether differential tariff should be introduced in a graded manner? If so, please suggest the methodology with justification.**

**TTL Response:** No Comments.

**TTL Additional Inputs:**

**A. Whitelisting SOP**

It is requested that TRAI should formulate a process for Blacklisted PE to appeal and file indemnification for whitelisting directly within defined SLA.



## **B. Digital Consent**

- In light of interpretation issues related to Service and Transactional Calls, consent acquisition becomes critical for complaint handling.
- PE are not coming forward for Digital Consent due to high-cost burden and cumbersome process therefore alternate ways can be identified like
- Entities to be allowed with directly feed of consent data to DLT, which they acquire during the onboarding process, when customers visit point of sales (POS), websites, applications, social media instead of only acquiring through DCA.
- TAPs to give option to their respective customers to monitor, modify and revoke the consents.

## **C. SPAM Tagging for 140XX numbers**

- As PE's are acquiring more and more 140XX resources, tagging of spam by application providers, handset manufacturers are hampering the success ration of calls originating from 140XX numbers. At the same time multiple attempts are made by such entities which in turn increases the network resource loading. Also, it is imposing issues in case of usage if recycled numbers and creating situation of number crunch within 140XX which is by default as spam by such application providers. It is requested to take suitable measures so that 140XX resources are effectively utilized.