Tanla Platforms Limited
Tanla Technology Centre,
Madhapur, Hyderabad,
Telangana, India - 500081
CIN: L72200TG1995PLC021262

+91-40-40099999
91-40-23122999
info@tanla.com
www.tanla.com

09-Oct-2024

To,
Shri. Jaipal Singh Tomar,
Advisor (QoS-II)
Telecom Regulatory Authority of India,
Jawaharlal Nehru Marg, Old Minto Road,
New Delhi – 110002

Subject: Submission on consultation paper on "Review of the Telecom Commercial Communications Customer Preference Regulations, 2018" Dated on: 28th Aug -2024.

Dear Sir,

Greetings from Tanla Platforms Limited.

Please find the enclosed comments of Tanla Platforms Limited on the above-mentioned consultation paper for your kind consideration.

Thanking You,

Yours sincerely,

Santhosh Kumar Posina
Vice President – Regulatory & Product Ops.
Santhosh.posina@tanla.com

tanla

Tanla Platforms Limited
Tanla Technology Centre,
Madhapur, Hyderabad,
Telangana, India - 500081
CIN: L72200TG1995PLC021262

+91-40-40099999
91-40-23122999
info@tanla.com
www.tanla.com

Q.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.

In paragraph 2.15, *Transactional Communication* is defined as any communication sent by the "Sender to its own customer or subscriber, excluding promotional communications." It is further clarified in the same paragraph that such communication may either be triggered by a subscriber-initiated transaction or stem from an ongoing relationship between the recipient and the Sender.
The first type, typically mandated by regulators such as the RBI for financial transactions, does not require the sender to provide an opt-out option to the subscriber. However, for the second type, where the communication is based on inferred consent due to an existing relationship, subscribers should have the right to opt out.

We recommend that these two types of communication be distinctly categorised as "Transactional Message" and "Service Message." This will ensure that the mandatory opt-out mechanism proposed by the Authority applies to the second category.

For instance, if a stock broker sends daily updates on the increase or decrease in a customer's portfolio value, such communication should be classified as *Service Communication* under these definitions, with a mandatory opt-out option.

Q.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.

Robocalls

A robocall is a phone call that uses an autodialer to deliver a pre-recorded message.
We agree with the suggestion in the consultation paper that robocalls should require prior consent of the subscriber, except when they are government calls (such as for emergency announcements) or transactional warnings (a detected fraud transaction attempt on a credit card). Such calls should only be allowed from 160 series.

Further, we recommend that pre-recorded content (payload) of the robocall should be stored on the DLT network and replayed by the concerned Access Provider.

Autodialers

They may be used for IVRS calls or other such calls that are completed by human or AI agents.

All such calls must be from 140 or 160 series, as appropriate, and have a mandatory pilot announcement about the nature of the call played to the recipient after the call is connected. This

announcement should be pre-recorded and include the name of the entity on whose behalf the call is made.

tanla

Tanla Platforms Limited
Tanla Technology Centre,
Madhapur, Hyderabad,
Telangana, India - 500081
CIN: L72200TG1995PLC021262

+91-40-40099999
91-40-23122999
info@tanla.com
www.tanla.com

The post connection pilot announcement should be served from the DLT network.
The user could also be given the option, if feasible, to decline the call by pressing standardised keys:

Press 1. To decline the call for now. (Repeat calls not possible for 30 minutes.)
Press 2. To decline the call and block further calls from the same caller.
Press 3. To register a complaint. The called party may record a short message after beep.

Q.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.

Pre-recorded calls should be scrubbed to verify the consent of the subscriber. The recorded content should be stored and served from the DLT network, as recommended for robocalls in response to Question 2 above.

This method aligns with best practices in other countries, such as the United States and the United Kingdom, where strict regulations govern the use of pre-recorded calls to ensure consumer protection and content control.

Q.4 Stakeholders are required to submit their comments in respect of Headers identifiers categories as suggested in the above paragraphs by the Authority 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.

The nature of a message is inherently revealed to the recipient by its content. Additionally, as highlighted in the consultation paper, Schedule-I of the TCCCPR 2018 mandates that Access Providers must prefix a label to the text of commercial communications, enabling recipients to easily identify whether the message is transactional, service-oriented, or promotional.

In line with this, we propose that the initial few characters of a registered message template should contain relevant metadata, such as the message type, in a standardised form and structure. This would free up the entire 11-character header space for Senders to effectively present their identity and the purpose of the message. Such an approach would also facilitate the grouping of related messages, enhancing ease of management for the recipient.

To maintain the integrity of this system, scrubbing services and firewalls must be configured to block any message, whether originating from a Registered Telemarketer (RTM) or Unregistered Telemarketer (UTM), that includes or imitates the reserved characters or structure. This is critical to prevent subscribers from being misled by unauthorised messages from spammers or fraudsters.

We further suggest that headers should only be registered after thorough scrutiny and that an "operator charge" be levied to discourage the indiscriminate creation of headers that do not provide

significant value to the Principal Entity (PE). The amount collected from this charge should be used to

tanla

Tanla Platforms Limited
Tanla Technology Centre,
Madhapur, Hyderabad,
Telangana, India - 500081
CIN: L72200TG1995PLC021262

+91-40-40099999
91-40-23122999
info@tanla.com
www.tanla.com

offset the costs borne by Terminating Access Providers (TAPs) in registering and investigating complaints. Therefore, we recommend that the operator charge be distributed among Access Providers, proportional to their subscriber base. The registration costs to the PE would comprise the operator charge and any fees that may be charged by the registrar.

The accounting for distribution of operator charges can be handled via the Contract API available on Hyperledger, using TRAI's latest subscriber data for each Access Provider.

We suggest a minimum operator charge of Rs. 5,000 per header per annum, to be collected by the registrar and distributed among Access Providers accordingly. The frequency of settlement and other procedural aspects could be left to be included in the relevant Code of Practice (CoP).

Q.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?

The current provisions for redress of consumers' complaints can be effective if properly enforced. However, to further improve the efficiency and effectiveness of the complaint handling process, we recommend leveraging automation across various stages of complaint redress.

Automation can streamline several critical processes, including:

1. **Basic Complaint Checks**: Automatically verifying complaints against mandatory and optional parameters to ensure completeness and accuracy.
2. **Instant Routing**: Immediate routing of complaints to the relevant Originating Access Provider (OAP) or Terminating Access Provider (TAP) based on predefined rules.
3. **DND Preference Validation**: Automatically cross-checking complaints against the subscriber's Do Not Disturb (DND) preferences to ensure valid grounds for the complaint.
4. **Time-based Validation**: Automatically validating whether the complaint falls within the stipulated time period after the Unsolicited Commercial Communication (UCC) was received.
5. **Call Detail Record (CDR) Validation**: Using automation to validate CDRs, ensuring that the details of the UCC are consistent with the complaint.
6. **Complaint Escalation**: Automated escalation of complaints to the relevant Enterprise, Registered Telemarketer (RTM), or Unregistered Telemarketer (UTM) for faster resolution.

By automation at these key stages, the complaint handling process can become more efficient, reducing human error and enabling faster, time-bound redress. Additionally, this approach will ensure timely identification of violators and assign responsibility appropriately, improving compliance and accountability across the ecosystem.

tanla

Tanla Platforms Limited
Tanla Technology Centre,
Madhapur, Hyderabad,
Telangana, India - 500081
CIN: L72200TG1995PLC021262

+91-40-40099999
91-40-23122999
info@tanla.com
www.tanla.com

Q.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. F. Financial Disincentives on Access Providers for failure to curb the UCC from registered Senders/RTMs

Proactive detection of Unsolicited Commercial Communication (UCC) can be implemented through two primary strategies:

Proactive Detection

1. **For Calls**: The phone calls that land on honeypots should be recorded and transcribed using speech-to-text technology. This is in addition to other signals that may be available, such as fan-out and duration of calls. The resulting text can then be analysed to flag potential spam content and take further action, as appropriate.
2. **For SMS**: The messages should be analysed using Artificial Intelligence (AI) and Machine Learning (ML) technologies.

All classification methods, irrespective of technology or human review, suffer from false positive filtration.

To address this, TRAI must periodically review the false positive and false negative rates achieved by different solutions deployed by the industry. It should thereafter set acceptable false positive thresholds for all AI/ML models to follow.

Honeypot Deployment Strategy

We urge the Authority to allocate the deployment of honeypots in proportion to the active subscriber base of each License Service Area (LSA). The current standard of one honeypot for every 200 complaints in the previous calendar year may be too low for larger LSAs with substantial subscriber numbers. To ensure wider coverage, we recommend deploying *honeypots at a rate of at least 0.05% of MSISDNs per LSA per Telecom Service Provider (TSP)*, allowing for a more extensive reach and better identification of malicious actors.

However, we request that the Authority reconsider treating data collected via honeypots as definitive proof of UCC violations. Such data should only be considered as evidence and evaluated in context. For instance, it is possible for an innocent caller to mis-dial the number of the intended recipient, thus landing on the honeypot. Any automatic action in response to such incidents would be unfair.

tanla

Tanla Platforms Limited
Tanla Technology Centre,
Madhapur, Hyderabad,
Telangana, India - 500081
CIN: L72200TG1995PLC021262

+91-40-40099999
91-40-23122999
info@tanla.com
www.tanla.com

Q.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 72 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

We propose the introduction of charges for the registration and annual maintenance of Templates, in the same manner as suggested for Headers. These should also be treated as "operator charges" and distributed to access providers in proportion to their subscriber base. The registrars may charge their own fees over and above such operator charges.

This system should not be viewed as a monetisation opportunity; rather, it serves to discourage mindless registration of templates, often for testing purposes, which are then left active in the system. Such unneeded templates (currently 90% remain unused indefinitely) become opportunities for spammers to hide their activities.

By attaching a value to the headers and content templates, the framework will naturally encourage the use of authentic and compliant templates, while discouraging non-compliant content. This approach will enhance adherence to the regulations and promote responsible use of commercial communications.