MyOperator
+91 92129 92129
hello@myoperator.com
www.myoperator.com
MyOperator, 91Springboard,
D-107, Sector 2, Noida, UP–201301

To,

Jaipal Singh Tomer,

Telecom Regulatory Authority of India,

F-Block, World Trade Center,

New Delhi-110029

Dear Sir,

At the outset, we would like to thank the Honourable Authority for issuing this important consultation paper, that will help ensure transparency, accountability, and adherence to regulatory standards. These elements are crucial for protecting consumer interests while giving a suitable environment for businesses.

Unsolicited calls to consumers must be stopped, and we appreciate the comprehensive approach taken in this paper regarding UCC and promotional calls. We are submitting our suggestions based on the questions and points raised in the paper.

However, we would like to highlight that the Honourable Authority is also aware of a distinct segment called "cloud telephony," which serves both large enterprises and MSMEs for business calls, primarily for transactional purposes. There are certain concerns related to this segment that hasn't been addressed in the paper.

In light of the above, aligned with the objective of bringing more transparency to promotional calls and the complaint mechanism, we have provided our responses to the questions asked in the paper.

Additionally, we would like to suggest a few amendments specifically for the cloud telephony segment to enhance its efficacy in Annexure 1.

Regards

Avneet Bhargava

Avneet Bhargava

VP-Operations

MyOperator

Annexure 1

Telecommunication has been playing a pivotal role in shaping the Indian economy by enabling not just large Business Enterprises but also MSMEs as a medium of growth. Any disruptive change that may impact the business ecosystem can disrupt the core objectives in the first place. While the objective is to control spam, it's important to recognize that only a small percentage of businesses engage in spamming, whereas most businesses utilize communication to reaching out to their customers for multifarious reasons.

Large portions of MSMEs have been using SIM cards for day-to-day business communication. As service providers, we have been putting our efforts to bring a lot of MSME to standard telecommunication platforms (Cloud Telephony) making business communication more digitized. We believe that the effort of such digitization should be further encouraged to provide supporting environments for MSMEs.

- Fee, Cost & Process of DLT Registration should be considered for MSMEs and should not be a reason for MSMEs to go back to SIM card calling.
- Penalties should be equitable for MSMEs and Large Enterprises. Having the same penalties for Enterprises and MSMEs may become a deterrent for MSMEs given their paying capacity is far below than that of an Enterprise.

Spam is not limited to telecommunications or India; it is a pervasive issue across various outreach platforms, including social media and advertising networks. Each platform has its own reporting systems and algorithms to combat spam, largely relying on user feedback. A spam score based on metrics would be beneficial, possibly facilitated by the DLT system. However again, considering the interest of MSMEs as well.

An example from the government's push for digital payments illustrates this approach. Instead of penalizing cash transactions, the government introduced user-friendly solutions like UPI and zero-balance accounts to encourage digital payment adoption. A similar strategy should be applied to telecommunications, easing processes for users.

We should draw an analogy for the DLT system from the financial sector, where all financial institutions use a centralized system called the Credit Information Bureau (India) Limited (CIBIL) framework, which allows them to check a person's credit score. Based on this score, they determine whether the user is genuine and decide the interest rate to charge on loans. The CIBIL score is calculated using information provided by banks based on a user’s financial history.

In the same way, DLT should function as a centralized system, where service provider can check the score of a particular principal entity before providing telecom resources. The principal entity would not need to register directly on the DLT; instead, their information, based on past telecom resources or MSME/GST records, would be available. This practice would help address the issues of spam and fraud effectively.

Encouragement to services providers would also bring a lot of MSME Communication to digital platforms. However, an inclusive platform allowing Service providers to participate in the process of spam control would help us partner in the whole process of Spam control and not be afraid of regulation ourselves.

- Recognize Cloud Telephony providers as service providers via simple registration as application service providers.
- Allow Service providers to submit the list of customers and their number during the time of KYC.
- Allow Service providers to Highlight/Submit Businesses blocked for Spamming on their platform accessible to every telco or access service provider

There are certain checks we as a platform are able to use to identify the Spam Caller from genuine ones and is based on few statistical models. Spam calls are likely to have significantly lower pickup rate along with shorter call length.

Challenges for MSME Category:

MSMEs often lack technical expertise. Most MSMEs use the TM's application directly, with the TM handling call generation and connecting them to their users. Although it has taken time to onboard MSMEs onto these technologies, if TRAI enforces the above process on the 160 series or transactional lines, MSMEs would start reverting to SIM card based calling which is the core reason for a lot of current challenges on both spam and scam. Some of the challenges MSMEs face include:

I. **Registration Charges**: Operators charge Rs 5,000 + GST annually for registration.
II. **Documentation Requirements**: Some basic documents are easily accessible, but operators may also request documents like an authorized signatory consent letter and board resolution, which MSMEs may not have, especially if they operate as sole proprietors.
III. **Template Registration**: Registering templates before making calls is complicated. MSMEs may not frequently use the DLT platform for logging in or updating information.
IV. **DID Procurement Process**: Obtaining a DID from DLT can take up to 48 hours, depending on the approval stages from the operator and TM. This process requires a thorough understanding of the DLT platform.
V. **Consent Acquisition under DCR**: Gaining user consent costs Rs 3 per user and requires significant knowledge of how to manage user consents. This process adds both a financial and operational burden for MSMEs.
VI. **No Incoming:** In the current 140 series solution, this is implemented only for outgoing calls, leading to MSMEs not adopt as is considered cost and friction in the communication.

Suggested Solutions:

1) **DLT Should Be Free for MSMEs**: The registration process should be simplified and cost-free for these businesses.
2) **TM Registration & third-party platforms**: TMs should be responsible for registering users on the DLT platform via API or Embedded processes.
3) **Simplified Consent Process**: MSMEs, being less familiar with the consent process, should not be burdened with it. Instead, they should be allowed to use resources freely, but if complaints arise, they can be evaluated based on a score (e.g., call patterns, short or bulk calls). If necessary, users can be suspended from the DLT platform by the TM, and this information should be shared with other operators.
4) **Template creation:-** Template creation should be easy and can be done via TM 's end as a integration too. TM will submit the template request as well as DID that is allocated by them.

We suggest looking at the Meta/WhatsApp AI approval process.

Meta follows a process for Whatsapp API Template approval where the TM (ISV/BSP incase of Meta) is sending the template approval request to the regulator for it's end customer. This eliminates the need for customer to directly interact with the regulatory body.

5) **DID allocation**:- TM and third party will use the API to allocate the DID.
6) **Spam check**: Spam check can be done via AI, E.g if a user is having pattern of less than 30 sec calls, or multiple complaints or previously blocked by any of the TM, AI can be built on these cases and can curb the spam and fraud at the same time.

Issues on consultation paper

Q1. Stakeholders are requested to submit their comments in respect of definitions of messages and calls and their categorizations, as suggested in paragraphs 2.14 to 2.19 along with necessary justifications.

Answer Transactional calls are made to convey information that is directly related to a transaction, service, or relationship that the recipient has with the business or entity.

Examples: Calls related to OTPs, service updates, account notifications, appointment reminders, delivery confirmations, feedback related to services and , Renewal dues

Key Characteristics:

- Informational in nature.
- Relevant to a service or transaction that the customer has opted into.

Promotional calls are made with the intent to promote a new product, service, or any offers to the recipient. These are typically commercial in nature and aimed at generating sales or customer engagement.

Examples: Calls offering discounts, advertising products, or promoting special deals.

Government Bodies calls- No comments

Q2. Whether explicit consent should be made mandatory for receiving promotional communications via auto dialer or robo calls? What other possible measures can be implemented to curb the use of auto dialer or robo calls without recipient consent? Stakeholders are requested to submit their suggestions, quoting best practices from around the world.

Answer:- Yes, consent is required for any promotional calls. As mentioned in Annexure 1, the consent process should be simple. MSMEs should be able to register consent on the DCR. The process should be straightforward and manageable either by the TM or the Principal Entity directly.Yes, consent is required for robo calls or pre-recorded messages, but the authority should differentiate between explicit and implicit consent. For instance, if a school needs to send a mass notification to parents due to an emergency or important information, this should fall under implicit consent. However, the current framework for explicit consent doesn't clearly differentiate between promotional and transactional notifications.

As a suggestion, while consent should be required, implicit consent should also be considered based on the use case, which can be approved by the telemarketer (TM).

To address the issue of auto-dialer or robo-calls, we can regulate the use and purpose of these calls under the DLT. However, since the 160 series is reserved only for the BFSI sector, this should be managed by the TM. For example, an auto call notification could be used to remind clients about their upcoming service renewals, children absent from the school notification to the parents, feedback related to quality of product delivered

Q3. As most pre-recorded calls have predefined content, stakeholders are requested to comment on the process to be followed for scrubbing such content before delivery to consumers. The comments should be supported with suitable justifications and practices from other parts of the world.

Answer:- There are a few suggestions, That are available in the world.

1) **Consent type**- Implicit and explicit consent based on their preference should be there
2) **Ease use of DLT**- DLT platform fee should be a minimum for uploading the consent, this will help PE to upload the consent.
3) **STIR/SHAKEN Equivalent for India**: TRAI could mandate the implementation of caller ID authentication technologies similar to the **STIR/SHAKEN** framework in the U.S. This would prevent call spoofing, ensuring that only authenticated and approved telemarketers can make calls.
4) **Caller Identity Transparency**: Mandate that all pre-recorded calls, especially promotional ones, clearly identify the sender, with the recipient being able to verify who is calling. This would make it easier for consumers to distinguish between legitimate and unsolicited calls.
5) **Use of AI**- Introduce a system where telecom providers automatically track and monitor consent levels for each telemarketer. This could help prevent unauthorized pre-recorded calls from being made to DND numbers
6) **Approval Process for Use Cases**: Similar to global practices, telemarketers should submit their use cases for approval by TRAI or an authorized body. For example, emergency notifications from schools or service renewal reminders could be pre-approved use cases.

Q4. Stakeholders are requested to submit their comments in respect of headers identifier categories, as suggested in paragraph 2.31 of Chapter II, or any other type of identifiers which may facilitate consumers to identify senders distinctly. Suggestions, if any, should be brought out with necessary justifications.

Answer:- We agree with Option 1.

Q5. Whether current provisions in the regulations for the redressal of consumer complaints in a time-bound manner are sufficient? If not, what provisions should be made for improving the effectiveness of complaint-handling processes, including identifying and fixing the responsibilities of the violators?

Answer- The current mechanism is effective, where service providers receive complaints and are required to provide opt-in proof as justification, if a Principal Entity (PE) (customers of service providers) makes a large number of calls to their customers and receives 1-2 complaints, this may simply indicate customer dissatisfaction with the services provided. However, this should not be considered a valid complaint if the PE is able to provide the necessary documentation.

In cases where the documentation is invalid or no justification is provided, it should be treated as a warning, and action should be taken in accordance with the law.

Q6. Whether the facilities extended by service providers through apps, websites, 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, websites, and call centres more accessible for registering UCC complaints and tracking their time-bound disposal? Please provide your answer with full details on the facilities needed.

Answer:- No currently not all Principle Entity has CCRF, This requires educating the Principal entity.

Q7. What additional modes of complaint registration, preference registration, and consent registration through easy and quick processes can be implemented?

Answer:- PEs/TMs should use incoming calls as a call centre for complaint registration, as it is easier to manage. However, in the current scenario, users prefer to file complaints via simple WhatsApp bots. PEs can now implement a WhatsApp-based process for handling UCC complaints.

Similarly, as per DCA guidelines, TRAI should recognize and accept consent obtained through WhatsApp, and this consent should be uploaded to the DLT platform.

This will streamline the process for providing and withdrawing consent efficiently.

Q8. Stakeholders are required to submit their comments on:

a) Measures required for proactive detection of spam messages and calls through honeypots and norms for their deployment.
b) Proactive actions needed to stop further communication of messages or calls identified as spam through UCC detection systems and actions against the senders.

Answer:- A) Proactive detection of spam messages and calls can be significantly enhanced through the deployment of honeypots, which are essentially decoy systems designed to attract and monitor suspicious activity. Here are the Key Mesaure and norms required for Honeypots

I. **Geographically dispersed deployment**- To capture a wise range of spam activity, deploy honeypots in different telecom cricle/server/ This will help esure locaized spam campaigns are also detected.
II. **AI detection system**- We need to educate our AI platform for honeypot for analyes the origin and nature of message or calls, This can include spam keyword analysis and number blacklisting.
III. **Data collections and analysis**- Deploy machine learning models to predict potential spam by analysin pattern and terns of the data collected. Like duration of calls, handup reason for calls.
IV. **Collaboration with telecom authorities**- Honeypot data should be shared with telecom regulators and service providers for blacklisting number and taking action against teh spammers.
V. **User Awareness Programs**: Based on the insights gathered from honeypots, develop user education programs to inform the public about evolving spam techniques and how to protect themselves.

b) To proactively stop further communication of messages or calls identified as spam through Unsolicited Commercial Communication (UCC) detection systems, several actions can be taken. These actions focus on preventing spam from reaching users and penalizing the senders to reduce future occurrences.

I. **Deploying Honeypots**: Set up honeypot numbers that intentionally attract spam messages and calls. These numbers help identify spam trends and patterns, and enable authorities to detect and block spam sources before they affect real users.
II. **Reputation-based Filtering**: Implement a reputation system that ranks numbers based on their past behavior. Numbers with a poor reputation due to spam activity can be subject to more stringent checks and restrictions.
III. **UTM and TM based filter**- In India, there are lots of company that are UTM but they are servicing to govt sector and public sector as a cloud telephony. There are chances that government identity might receive some complaint or may be public sector, such UTM should give a fair chance to justify the complaint and resolve with particular PE and submit the report to TSP and TRAI on time to time.

Q9. Stakeholders are required to submit their comments on:

- (a) Financial disincentives proposed in Section F of Chapter II for access providers against violations by RTMs.
- (b) Financial disincentives proposed in Section F of Chapter II for access providers against violations by UTMs.
- (c) Financial disincentives against the wrong approval of headers and message templates proposed in Section F of Chapter II on the access providers.
- (d) Measures needed to assign responsibilities to telemarketers (both RTMs and UTMs) and principal entities (senders) involved in sending UCC, and disincentivizing them financially, including legal actions as per law.

Answer(A to C) :- Penalties for valid UCC violations or misreported UCC cases, as outlined in Section F, sound appropriate. However, it's important to clearly define what constitutes a valid UCC before applying any penalties. A valid UCC should refer to a case where a call or SMS was sent to a user without their consent. Consent should be documented and available in digital form.

Imposing penalties without first seeking justification could lead to false UCC reports, either unintentionally or deliberately by users. For UTM or service provider, which are not yet integrated into the DLT system due to the nature of their business and calls, UCC complaints should be verified by them. UTMs should request documentation from the Principal Entity (PE) to substantiate their case. If there are repeated complaints or the spam threshold is exceeded, the UTM should act by blocking the PE and informing TRAI and the TSP.

There should also be a tool that allows UTMs/TM to report such actions to TRAI and the TSP to ensure proper documentation and tracking of these cases.

d) To effectively combat Unsolicited Commercial Communication (UCC), it is crucial to assign clear responsibilities to **service provider** (both Registered Telemarketers (RTMs) and Unregistered Telemarketers (UTMs)) and **Principal Entities (PEs)** (the actual message/call senders), while implementing financial disincentives and legal actions. Here are the measures needed to achieve this:

1. Clear Assignment of Responsibilities

- **Telemarketers (RTMs & UTMs)**:
  - **Compliance with Regulations**: Telemarketers must strictly adhere to regulations set by authorities like TRAI (Telecom Regulatory Authority of India) or the relevant body. This includes using only registered channels for communication and complying with the guidelines for sending commercial messages/calls.
  - **Verification of Consent**: Telemarketers are responsible for ensuring that every communication sent on behalf of a Principal Entity is consent-based. They should have systems in place to verify and store opt-in consent from users in a digital, auditable format.
  - **Reporting Mechanism**: RTMs and UTMs must regularly report their call/message volumes and complaint rates to the regulatory body and the telecom service provider (TSP). This reporting should include data on any UCC-related issues and resolutions.
  - **Monitoring and Auditing**: Regular audits should be conducted by TSPs or regulatory bodies to ensure telemarketers are not sending spam or bypassing regulations.
- **Principal Entities (PEs)**:
  - **Ownership of Consent Data**: PEs (the actual businesses sending the messages or calls) must be responsible for obtaining and maintaining users' consent to receive communications. They must ensure that telemarketers use the data appropriately.
  - **Regular Review of Telemarketers**: PEs should regularly review the practices of the telemarketers they hire to ensure compliance with UCC regulations. They must have clear agreements that outline consequences for non-compliance.
  - **Liability for Misuse**: PEs should be held accountable if their telemarketers misuse their database for UCC. This includes financial penalties or legal actions if found guilty of allowing unsolicited communication.

2. Financial Disincentives for Non-Compliance

- **Monetary Penalties for UCC Violations**:
  - For each valid UCC violation (where communication occurred without consent), RTMs, UTMs, and PEs should be subjected to increasing fines based on the severity and frequency of the offenses. For example, penalties could escalate for repeated offenses, such as ₹5,000 for the first violation(for a valid complaint where obtain proof are not available or digital consent is not available), ₹10,000 for the second, and so on.
  - A cap on the number of warnings before penalties escalate could be implemented, discouraging repeated violations.
- **Forfeiture of Security Deposits**:
  - RTMs should maintain a security deposit with TSPs. In cases of serious or repeated violations, part or all of this deposit can be forfeited as a financial disincentive.
  - PEs that regularly engage in spam activity should also be required to provide a security deposit, which may be forfeited for UCC violations.
- **Increased Transactional Costs for Non-Compliance**:
  - Telemarketers who fail to adhere to UCC guidelines could face higher per-message or per-call fees imposed by the TSP, making non-compliance financially unattractive.

4. Monitoring, Reporting, and Enforcement

- **Centralized Monitoring Platform**:
  - A centralized platform, managed by the regulatory body, should be established to monitor UCC complaints, reports, and actions taken. Both telemarketers and PEs should be required to submit data to this platform.
  - Real-time monitoring of UCC traffic and user complaints can help identify problem areas quickly and take swift action against offenders.
- **Complaint Resolution Timeline**:
  - Regulatory bodies should set strict timelines for investigating and resolving UCC complaints. For instance, every UCC complaint should be investigated within 10 working days, and corrective action should be implemented immediately after confirmation.
- **Random Audits and Spot Checks**:
  - Conduct random audits and spot checks on RTMs, UTMs, and PEs to ensure compliance. Failure to cooperate with an audit or inspection should result in penalties or suspension of operations.

5. Education and Awareness

- **Industry Education Programs**:
  - Conduct regular training and awareness sessions for RTMs, UTMs, and PEs on their responsibilities under UCC regulations, the penalties for violations, and the best practices for obtaining and maintaining user consent.
- **User Awareness**:
  - Launch campaigns to educate users on how to report UCC violations and how to protect themselves from unsolicited communications. This will help increase complaint accuracy and reduce false reports.

6. Use of Technology for Better Compliance

- **DLT System Integration**:
  - Ensure that all RTMs and UTMs are integrated into a Distributed Ledger Technology (DLT) system, where consent and transactional history are recorded transparently and tamper-proof. This helps track communication legitimacy.
- **Automated Compliance Tools**:

Telemarketers should implement automated systems that flag potential UCC violations and ensure communications are compliant before they are sent.

Q10. Whether there is a need to review the five-paisa exemptions for transactional messages and bring them on par with other commercial messages? If yes, please provide 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?

Answer:- Yes, this can be considered, but TSPs need to ensure that templates are approved based on variables, and these variables should not exceed their limits. Currently, this is an effective method to stop spammers. Additionally, once the Principal Entity (PE) submits a message, Telemarketers (TM) can use AI to analyze the content and block messages based on keywords and data from past trends.

Q11. 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 Procedures (SOPs) further, to enable access providers to take actions including imposing financial disincentives and legal actions against entities not following the regulations?
- (b) Whether there should be a provision for minimum security deposits from entities registering with any of the access providers, to prevent misuse or breaches of regulations? If so, what should be the provisions for encashment/replenishment of these deposits against violations of regulations?

Answer:- a) Yes, there is a need to strengthen the provisions of the Common Code of Practice templates by introducing more robust **Standard Operating Procedures (SOPs)**. Strengthening these provisions would empower access providers to take more decisive actions, including imposing financial disincentives and pursuing legal actions against entities that do not comply with the regulations. SOPs should include

- Clear definition of Role and Responsibilities
- Escalation Mechnanisam
- Template approval process
- Escalation for repeat offenders
- Blacklist mechanism
- Frequent audits

b) Introducing a **minimum security deposit** for entities registering with access providers creates a strong financial incentive for compliance and serves as a safeguard against regulatory breaches. Provisions for **encashment** and **replenishment** should be clearly defined, based on the severity and frequency of violations, to ensure that this measure effectively deters misuse while maintaining fair opportunities for entities to rectify their behavior.

Q12. What effective steps can be taken to control the menace of UCC through tariffs? Please justify your answer.

Answer :- No comments, details mentioned in Annexure 1

Q13. Whether differential tariffs for SMS and voice calls beyond a certain limit should be introduced to disincentivize UCC through UTMs? Please justify.

Answer:- No comments

Q14. If differential tariffs are introduced, what should be the limit beyond which they would apply for:

- (a) Voice calls.
- (b) SMS.
- Please justify with rationale.

Answer:- No Comments, Details mentioned in Annexure 1

Q15. If differential tariffs are introduced, what should be the tariff beyond a certain limit for:

- (a) Voice calls.
- (b) SMS.
- Please justify with rationale.

Answer: No Comments

Q16. Should differential tariffs be introduced in a graded manner? If so, please suggest the methodology with justification.

Answer:- NA.