VNO Response:

Based on the detailed categorization provided for commercial communications, here are some suggestions for refining and implementing the categories:

1. Transactional Messages or Transaction Calls

Definition and Scope:

Definition: Communications sent by a Sender to its own customer or subscriber that are necessary for transactions or services, excluding any promotional content.

Purpose: To provide essential information related to transactions or services that the recipient has engaged in or is in an ongoing relationship with the Sender.

- **Implementation Suggestions:**

1. **Template Clarity:** Ensure that the content of transactional messages is clearly distinguishable from promotional content to avoid confusion.
2. **Opt-Out Mechanism:**
o **Inclusion:** Include an opt-out option in every transactional message or call. This should be clearly stated and easily actionable.
o **Visibility:** The opt-out option should be prominently visible and simple to execute.
3. **Revocation Handling:**
o **DL-Consent Management:** Maintain and regularly update a centralized list of opted-out recipients to ensure compliance.
o **Re-consent Timing:** Implement a 90-day waiting period before soliciting re-consent to prevent frequent consent requests and respect user preferences.

2. Promotional Messages or Promotional Calls

Definition and Scope:

- **Definition:** Communications that contain advertisements or promotional material about products or services.
- **Purpose:** To market or promote products or services to potential or existing customers.

Implementation Suggestions:

1. **Consent Management:**
o **Digital Consent Acquisition (DCA):** Use a robust DCA system to obtain and manage explicit digital consent. Ensure that this system is secure and compliant with privacy regulations.

- o   **Preference Adherence:** Honor registered preferences and provide a mechanism for users to update their consent preferences easily.
- o
2. **Transparency:**
- o   **Clear Identification:** Make it clear when a communication is promotional to differentiate it from transactional or government communications.
- o   **Consent Revocation:** Allow users to opt-out of promotional communications easily and ensure this is processed promptly.

3. Government Messages or Government Calls

Definition and Scope:

- •   **Definition:** Communications sent at the direction of government authorities or statutory bodies for public interest purposes.
- •   **Purpose:** To convey important information or instructions that serve public welfare or legal requirements.

Implementation Suggestions:

1. **Identification:**
- o   **Clear Marking:** Clearly mark government communications as such to distinguish them from other types of messages.
- o   **Standard Templates:** Use standardized templates for government communications to ensure consistency and clarity.
2. **Blocking and Opt-Out:**
- o   **Non-Blockable:** Ensure that recipients cannot block government messages to maintain the effectiveness of these communications.
- o   **No Opt-Out Required:** Maintain the policy that explicit consent is not required for government messages, but ensure that the communications are relevant and necessary.

Additional Considerations:

1. **Regulatory Compliance:**
- o   Regularly review and update policies to comply with evolving regulations and industry standards.
- o   Engage with stakeholders to ensure that the implementation of these categories aligns with legal and consumer protection requirements.
2. **User Experience:**
- o   Prioritize a user-friendly approach for managing consent and preferences. This includes clear instructions for opting in or out and straightforward methods for users to exercise their choices.
3. **Data Security and Privacy:**
- o   Implement strong data protection measures to safeguard user information, especially when handling consent and preference data.
- o   Ensure transparency in how user data is used and provide users with control over their information.

By adopting these suggestions, you can help ensure that the categorization and management of commercial communications are clear, effective, and respectful of user preferences and regulatory requirements.

Q2.   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.

VNO Response:

To address the issue of auto-dialer or robo calls and the need for explicit consent, here are some insights and best practices that can be considered:

1. Explicit Consent for Promotional Communications

Recommendation: Yes, explicit consent should be mandatory for receiving promotional communications by auto-dialer or robo calls. Here's why:

- **Consumer Protection:** Explicit consent ensures that recipients have willingly opted in to receive such communications, protecting them from unsolicited calls.
- **Regulatory Compliance:** Many countries have stringent regulations requiring explicit consent for marketing communications to prevent spam and intrusive calls.
- **Enhanced Trust:** Obtaining explicit consent fosters trust between businesses and consumers, improving customer relations and brand reputation.

2. Best Practices for Managing Auto-Dialer and Robo Calls

A. Obtain Explicit Consent

1. **Clear Opt-In Procedures:**
o   **Consent Forms:** Implement clear and user-friendly consent forms where individuals can voluntarily opt in to receive promotional calls. These forms should clearly explain what type of calls they are consenting to receive.
o   **Digital Verification:** Use digital channels for consent, such as through online forms, text messages, or email confirmations, ensuring the process is secure and verifiable.

2. **Confirmation Process:**
o **Double Opt-In:** Implement a double opt-in process where after initial consent, a confirmation step is required to verify the user's intention. This minimizes the risk of accidental or fraudulent consents.

B. Implementing Measures to Curb Unwanted Calls

1. **Regulation and Enforcement:**
o **Strict Regulations:** Enforce strict regulations that prohibit auto-dialer and robo calls without explicit consent. Regulations should include heavy penalties for non-compliance.
o **National Do Not Call Lists:** Establish and maintain national Do Not Call lists where consumers can register their preference to avoid unsolicited marketing calls.
2. **Technological Solutions:**
o **Call Blocking Technology:** Promote the use of call-blocking technologies and applications that can identify and block unsolicited auto-dialer or robo calls.
o **Caller ID Authentication:** Implement caller ID authentication systems to verify the legitimacy of the caller, reducing the effectiveness of spoofed or fraudulent calls.
3. **Transparent Reporting Mechanisms:**
o **Complaint Channels:** Create transparent and accessible channels for consumers to report unwanted calls. Ensure these complaints are reviewed and acted upon promptly.
o **Monitoring and Audits:** Regularly monitor and audit communication practices to ensure compliance with consent requirements and regulations.
4. **Public Awareness Campaigns:**
o **Educate Consumers:** Conduct awareness campaigns to educate consumers about their rights regarding unsolicited calls and how to report them.
o **Inform Businesses:** Provide guidance and training to businesses on best practices for obtaining consent and managing auto-dialer systems.

C. International Best Practices

1. **United States:**
o **Telephone Consumer Protection Act (TCPA):** Requires explicit consent before making auto-dialed or prerecorded calls to mobile phones and establishes a National Do Not Call Registry.
o **National Do Not Call Registry:** Allows consumers to opt out of receiving unsolicited telemarketing calls.
2. **European Union:**
o **General Data Protection Regulation (GDPR):** Requires explicit consent for direct marketing communications and has stringent rules on data processing and user consent.
o **ePrivacy Directive:** Addresses the use of auto-dialers and unsolicited calls, ensuring that consent is obtained before such communications.

3. **Australia:**
o   **Do Not Call Register Act:** Provides a Do Not Call Register where consumers can opt out of receiving unsolicited telemarketing calls.
o   **Spam Act:** Regulates the sending of unsolicited commercial electronic messages, including calls.
4. **Canada:**
o   **Canada's Anti-Spam Legislation (CASL):** Requires explicit consent for sending commercial electronic messages, including calls, and enforces penalties for non-compliance.

Conclusion

To effectively manage and curb the use of auto-dialer or robo calls without consent:

- **Mandate explicit consent** for all promotional communications.
- **Enhance regulatory frameworks** to address and penalize non-compliance.
- **Leverage technology** to identify and block unsolicited calls.
- **Establish robust complaint and reporting systems**.
- **Promote public awareness** and ensure businesses are well-informed about compliance requirements.

By implementing these practices and drawing on global best practices, stakeholders can help protect consumers from unwanted calls and improve the overall communication environment.

Q3.   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.

VNO Response:

Address the challenge of scrubbing pre-recorded content before delivery to consumers, stakeholders should consider implementing a robust process to ensure compliance with regulations, respect for consumer preferences, and protection from unwanted communications. Here's a comprehensive approach, supported by justifications and international practices:

1. Content Scrubbing Process

A. Content Approval and Verification

1. **Pre-Approval Process:**
o   **Content Review:** Establish a pre-approval process where all pre-recorded content must be reviewed and approved before being used for calls. This includes verifying that the content aligns with legal requirements and is appropriate for the intended audience.

o **Compliance Check:** Ensure that content complies with local regulations, such as the requirement for explicit consent, and does not include misleading or deceptive information.

2. **Content Certification:**

o **Certification Systems:** Implement a certification system where content must be certified by a regulatory body or an internal compliance team to confirm that it meets all regulatory and ethical standards.

o **Documentation:** Maintain detailed records of content approval and certification for audit purposes.

B. Opt-Out and Consent Management

1. **Integration with Consent Databases:**

o **Database Integration:** Integrate content delivery systems with opt-out and consent databases to ensure that pre-recorded content is not sent to individuals who have opted out or have not provided explicit consent.

o **Real-Time Verification:** Implement real-time verification of consent status before initiating calls to ensure compliance with preferences.

2. **Dynamic Content Adaptation:**

o **Adaptive Content:** Use technology to dynamically adapt pre-recorded content based on the recipient's consent status and preferences. This helps avoid sending content to those who have opted out or have specific communication preferences.

C. Monitoring and Auditing

1. **Regular Audits:**

o **Compliance Audits:** Conduct regular audits of pre-recorded content and delivery processes to ensure ongoing compliance with regulations and internal policies.

o **Random Checks:** Implement random checks on pre-recorded calls to verify adherence to approved content and consent requirements.

2. **Feedback Mechanism:**

o **Consumer Feedback:** Establish a mechanism for consumers to provide feedback or report issues with pre-recorded calls. Use this feedback to continuously improve content management processes.

D. Transparency and Accountability

1. **Clear Disclosure:**

o **Disclosure Information:** Ensure that pre-recorded calls include clear disclosure about the nature of the call, the identity of the caller, and the purpose of the communication. This transparency helps maintain consumer trust and ensures compliance with regulations.

o **Opt-Out Options:** Provide easy and immediate options for recipients to opt out of further communications during the call.

2. Justifications and International Practices

A. Justifications:

1. **Consumer Protection:**

o   **Respect for Preferences:** Scrubbing content before delivery ensures that communications respect consumer preferences and opt-out requests, reducing the likelihood of complaints and regulatory violations.

o   **Avoiding Misuse:** Pre-approval and compliance checks prevent the misuse of auto-dialers and robo-calls, protecting consumers from intrusive or fraudulent communications.

2. **Regulatory Compliance:**

Legal Adherence: Adhering to pre-approval and scrubbing processes helps ensure compliance with regulations governing unsolicited communications and consent requirements, avoiding legal penalties.

   Trust Building:

o   **Transparency:** Transparent processes and clear disclosures build trust with consumers, enhancing the reputation of businesses and reducing consumer dissatisfaction.

B. International Practices:

1. **United States:**
o   **Telephone Consumer Protection Act (TCPA):** Requires pre-recorded calls to obtain prior express consent and prohibits calls to numbers on the National Do Not Call Registry. The Federal Communications Commission (FCC) enforces these rules and requires accurate record-keeping.

o   **Robocall Mitigation:** The TRACED Act mandates that carriers implement call authentication technologies to prevent fraudulent robocalls.

2. **European Union:**
o   **General Data Protection Regulation (GDPR):** Requires explicit consent for marketing communications, including pre-recorded calls. The GDPR also mandates that organizations maintain records of consent and provide mechanisms for consumers to withdraw consent.

o   **ePrivacy Directive:** Regulates the use of automated calling systems and requires that consent be obtained before making such calls.

3. **Australia:**
o   **Do Not Call Register Act:** Prohibits unsolicited telemarketing calls to numbers registered on the Do Not Call Register. Businesses must scrub their call lists against this register.

o   **Spam Act:** Requires consent for commercial electronic messages and mandates that businesses provide opt-out options and honor opt-out requests.

4. **Canada:**
o   **Canada's Anti-Spam Legislation (CASL):** Requires explicit consent for sending commercial electronic messages, including pre-recorded calls. Organizations must maintain records of consent and provide clear opt-out options.

Conclusion

To effectively manage pre-recorded content and ensure compliance:

- **Implement a rigorous content approval process** that includes pre-approval and certification.
- **Integrate consent databases** to prevent unauthorized communications.
- **Conduct regular audits** and use feedback mechanisms to ensure adherence to regulations and improve processes.
- **Adopt international best practices** to ensure that content scrubbing processes align with global standards and enhance consumer protection.

By following these recommendations, stakeholders can help reduce the misuse of auto-dialers and robo-calls, ensuring a more respectful and compliant communication environment.

Enhance transparency and allow consumers to identify senders more distinctly, it's essential to implement effective header identifiers or similar mechanisms. Here's a structured approach to header identifiers and other methods that can facilitate clearer identification of senders:

1. Header Identifiers Categories

A. Proposed Categories of Header Identifiers:

1. **Sender Name and Brand Identification:**
o **Description:** Display the name or brand of the sender prominently in the header.
o **Justification:** Helps recipients immediately recognize who is contacting them, reducing confusion and potentially fraudulent messages.
o **Example:** "ABC Bank" or "XYZ Store"
2. **Communication Type Indicator:**
o **Description:** Include a tag indicating the type of communication, such as "Transactional," "Promotional," or "Government."
o **Justification:** Provides context about the nature of the message, allowing recipients to prioritize or filter communications.
o **Example:** "[Transactional]" or "[Promotional]"
3. **Sender Contact Information:**
o **Description:** Include contact information or a verified sender ID in the header.
o **Justification:** Offers a way for recipients to verify the authenticity of the sender and respond if needed.
o **Example:** "Call us at 1800-123-4567"
4. **Unique Sender Identifier:**
o **Description:** Assign a unique identifier (such as a number or code) to each sender, which can be cross-referenced with a database.
o **Justification:** Enables easy identification and verification of senders, especially in automated systems.
o **Example:** "SenderID: 12345"
5. **Verification Badge or Logo:**
o **Description:** Display a verification badge or logo indicating that the sender has been authenticated.
o **Justification:** Enhances trust and confidence in the authenticity of the communication.
o **Example:** A small checkmark or verified logo.

B. Implementation Considerations:

1. **Standardization:**
o   **Description:** Develop and adopt standardized formats for header identifiers to ensure consistency across communications.
o   **Justification:** Consistency allows for easier recognition and handling of communications by recipients and service providers.
2. **Regulatory Compliance:**
o   **Description:** Ensure that header identifiers comply with local and international regulations governing electronic communications and privacy.
o   **Justification:** Prevents legal issues and ensures that the system meets regulatory requirements.
o

2. Alternative Methods for Sender Identification

A. Enhanced Sender ID Systems:

1. **Verified Sender Database:**
o   **Description:** Maintain a centralized database of verified senders, with details accessible to recipients.
o   **Justification:** Allows recipients to look up and verify senders, enhancing trust and reducing fraud.
o   **Example:** A web portal where recipients can check the legitimacy of the sender.
2. **Caller ID Authentication:**
o   **Description:** Implement technologies for authenticating caller ID for voice communications.
o   **Justification:** Helps prevent spoofing and ensures that the caller ID matches the actual sender.
o   **Example:** STIR/SHAKEN framework for voice calls.

B. Consumer Education and Tools:

1. **Education Campaigns:**
o   **Description:** Run campaigns to educate consumers on recognizing legitimate communications and using available tools to verify senders.
o   **Justification:** Empowers consumers to make informed decisions and recognize potential fraud.
o   **Example:** Guides on identifying phishing attempts or fraudulent communications.
2. **Filtering and Blocking Tools:**
o   **Description:** Develop and promote tools that allow consumers to filter or block communications from unknown or suspicious senders.
o   **Justification:** Provides consumers with control over the types of communications they receive.
o   **Example:** Mobile apps or software that block suspected spam or fraud calls.

3. International Best Practices

A. United States:

- **STIR/SHAKEN Framework:** This framework for phone call authentication helps combat caller ID spoofing and ensures that calls are correctly identified.
- **Caller ID Authentication:** Utilizes standards and protocols to verify the authenticity of caller IDs.

B. European Union:

- **ePrivacy Regulation:** Includes provisions for identifying and authenticating communications, ensuring that users are aware of the nature of the calls or messages they receive.

C. Australia:

- **Do Not Call Register:** Maintains a national registry to help consumers avoid unsolicited calls and provides clear identification for legitimate callers.

D. Canada:

- **Canada's Anti-Spam Legislation (CASL):** Requires clear identification of senders in commercial electronic messages and mandates consent before sending such messages.

Conclusion

To improve the identification of senders and enhance consumer trust:

1. **Adopt a standardized set of header identifiers** that includes sender name, communication type, contact information, and verification badges.
2. **Implement additional verification systems** such as a verified sender database and caller ID authentication technologies.
3. **Promote consumer education** on identifying legitimate communications and using tools for filtering and blocking unwanted messages.

By adopting these practices, stakeholders can improve transparency, reduce fraud, and enhance the overall communication experience for consumers.

Q4. 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?

VNO Response:

To assess and improve the effectiveness of complaint redressal provisions in regulations, it's important to examine both current provisions and potential enhancements. The goal is to ensure that complaints are addressed promptly and that

violators are held accountable. Here's a detailed analysis and suggestions for improvement:

1. Current Provisions for Redressal

A. Existing Mechanisms:

1. **Complaint Submission:** Typically, regulations require that consumers be able to submit complaints through designated channels such as online portals, hotlines, or email.
2. **Acknowledgment and Tracking:** There should be a system for acknowledging receipt of complaints and tracking their status.
3. **Resolution Timeframes:** Regulations often specify timeframes within which complaints must be resolved (e.g., 7 to 30 days).
4. **Escalation Processes:** There are usually provisions for escalating complaints if they are not resolved satisfactorily within the stipulated timeframe.
5. **Penalties for Violators:** Regulations may include penalties for entities found to be in violation of the rules, but enforcement mechanisms can vary.

2. Analysis of Current Provisions

A. Limitations and Gaps:

1. **Timeliness:** Some regulations may have insufficient timeframes or lack stringent enforcement mechanisms to ensure timely resolution.
2. **Transparency:** Lack of transparency in the complaint handling process can lead to dissatisfaction among consumers.
3. **Accountability:** Identifying and fixing responsibilities for violators can be challenging, particularly if enforcement mechanisms are weak or poorly implemented.
4. **Consistency:** There may be inconsistencies in how complaints are handled across different entities or regions.

3. Recommendations for Improvement

A. Enhancing Timeliness:

1. **Shorter Resolution Timeframes:**
o   **Recommendation:** Implement shorter, more stringent timeframes for resolving complaints (e.g., 5 to 10 days) to ensure prompt action.
o   **Justification:** Faster resolution helps maintain consumer trust and reduces the backlog of unresolved complaints.
2. **Automated Tracking Systems:**
o   **Recommendation:** Develop automated tracking systems to provide real-time updates on the status of complaints.
o   **Justification:** Automation increases efficiency and provides transparency to consumers about the progress of their complaints.

B. Improving Transparency:

1. **Clear Communication:**

o   **Recommendation:** Ensure that consumers receive regular updates and clear explanations about the status and outcome of their complaints.

o   **Justification:** Transparency builds trust and keeps consumers informed about the resolution process.

2. **Public Reporting:**

o   **Recommendation:** Publish periodic reports on complaint statistics, common issues, and resolution outcomes.

o   **Justification:** Public reporting enhances accountability and provides insights into systemic issues that may need addressing.

C. Strengthening Accountability:

1. **Clear Responsibilities:**

o   **Recommendation:** Define and communicate clear responsibilities for complaint handling within organizations, including assigning specific roles and accountability.

o   **Justification:** Clear responsibilities ensure that there is no ambiguity about who is accountable for resolving complaints.

2. **Penalties and Enforcement:**

o   **Recommendation:** Implement more robust enforcement mechanisms, including higher penalties for non-compliance and frequent audits of complaint handling processes.

o   **Justification:** Effective enforcement ensures that entities take their complaint handling obligations seriously.

D. Enhancing Complaint Handling Processes:

1. **Training and Resources:**

o   **Recommendation:** Provide regular training and resources for staff handling complaints to ensure they have the skills and knowledge needed to resolve issues effectively.

o   **Justification:** Well-trained staff are better equipped to handle complaints efficiently and fairly.

2. **Consumer Empowerment:**

o   **Recommendation:** Offer tools and resources that empower consumers to understand their rights and navigate the complaint process effectively.

o   **Justification:** Empowering consumers helps them make informed decisions and increases the effectiveness of the complaint process.

E. Technological Integration:

1. **Digital Platforms:**

o   **Recommendation:** Utilize digital platforms and mobile apps to streamline the complaint submission and tracking process.

o   **Justification:** Digital platforms can make the complaint process more accessible and user-friendly.

2. **Data Analytics:**

o   **Recommendation:** Use data analytics to identify trends, monitor performance, and address recurring issues.

o   **Justification:** Analytics help in understanding patterns and improving overall complaint handling processes.

4. International Best Practices

A. United States:

• **Consumer Financial Protection Bureau (CFPB):** Utilizes an online complaint portal with tracking and status updates. The CFPB also publishes complaint data for transparency.

B. European Union:

• **European Consumer Centre (ECC) Network:** Provides a centralized platform for consumers to submit complaints and offers mediation services.

C. Australia:

• **Telecommunications Industry Ombudsman (TIO):** Offers a structured complaint resolution process with clear timelines and escalation procedures.

D. Canada:

• **Canadian Radio-television and Telecommunications Commission (CRTC):** Implements robust complaint handling processes with clear timelines and public reporting.

Conclusion

To enhance the effectiveness of complaint handling processes:

1. **Adopt shorter resolution timeframes** and **automated tracking systems** for efficiency.
2. **Ensure clear communication** and **publish public reports** for transparency.
3. **Define clear responsibilities**, **implement robust penalties**, and **strengthen enforcement mechanisms** for accountability.
4. **Invest in training**, **empower consumers**, and **leverage technology** to improve the overall process.

By implementing these recommendations, stakeholders can improve the complaint redressal system, ensuring that consumer complaints are handled efficiently, transparently, and fairly.

Q5.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 takenby the service providers to make their Apps, Website and Call Centres 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 thefacilities needed.

VNO Response:

Evaluation of Current Facilities for Handling Unsolicited Commercial Communications (UCC) Complaints

1. **Accessibility and Consumer-Friendliness of Current Facilities:**

A. Apps, Websites, and Call Centers:

- **Apps:**
o **Strengths:** Mobile apps offer convenience, allowing users to report complaints directly from their phones. They often provide features like push notifications and real-time tracking.
o **Weaknesses:** Some apps may be difficult to navigate, lack comprehensive features, or have limited accessibility options for users with disabilities.
- **Websites:**
o **Strengths:** Websites provide a broad range of resources and may include detailed instructions on how to file complaints. They often have extensive FAQs and support sections.
o **Weaknesses:** Websites can be cluttered, not mobile-friendly, or difficult to navigate. Accessibility issues may affect users with disabilities.
- **Call Centers:**
o **Strengths:** Call centres offer direct human interaction, which can be helpful for resolving complex issues or for users who prefer speaking with a representative.
o **Weaknesses:** Long wait times, complex automated menus, and language barriers can make call centres less user-friendly.

B. Current Facilities Review:

- **Accessibility:** Many current systems may not fully comply with accessibility standards (e.g., WCAG 2.1 for websites) and may not cater to users with disabilities.
- **Ease of Use:** Users often face difficulties with complicated menus, insufficient guidance, and lack of real-time updates on complaint status.

2. Recommended Improvements

A. Enhancing Accessibility and Usability:

1. **Unified Complaint Management System:**
o **Recommendation:** Develop a unified complaint management system accessible through apps, websites, and call centres.
o **Justification:** A unified system ensures consistency in handling complaints and provides a single point of access for users.
2. **User-Friendly Design:**
o **Recommendation:** Design apps and websites with user-friendly interfaces, incorporating intuitive navigation and clear instructions.
o **Justification:** A user-friendly design reduces frustration and helps users easily find and use the complaint submission features.
3. **Accessibility Features:**
o **Recommendation:** Ensure compliance with accessibility standards, including screen reader compatibility, text-to-speech options, and high-contrast modes.
o **Justification:** Accessibility features are essential for users with disabilities and ensure that all consumers can access the complaint registration and tracking services.
4. **Multilingual Support:**
o **Recommendation:** Provide support in multiple languages to cater to diverse consumer demographics.
o **Justification:** Multilingual support helps non-native speakers file complaints more easily and improves overall user experience.

B. Improving Complaint Registration and Tracking:

1. **Streamlined Registration Process:**
o **Recommendation:** Simplify the complaint registration process with a step-by-step guide and easy-to-fill forms.
o **Justification:** A streamlined process reduces barriers to filing complaints and ensures that users can quickly and efficiently report UCC issues.
2. **Real-Time Tracking and Updates:**
o **Recommendation:** Implement real-time tracking of complaints with notifications and updates at each stage of the process.
o **Justification:** Real-time tracking keeps users informed about the status of their complaints and helps manage their expectations.
3. **Automated Acknowledgments and Responses:**
o **Recommendation:** Use automated systems to send acknowledgments upon receipt of complaints and provide estimated resolution times.
o **Justification:** Automated responses reassure users that their complaints have been received and provide an initial timeline for resolution.
4. **Feedback and Escalation Mechanisms:**
o **Recommendation:** Include options for users to provide feedback on the complaint handling process and escalate unresolved issues to higher authorities.
o **Justification:** Feedback mechanisms help improve the process, while escalation options ensure that unresolved issues receive further attention.

C. Call Center Enhancements:

1. **Improved Automated Menus:**
o **Recommendation:** Design automated phone menus to be simple and intuitive, reducing the need for users to navigate complex options.

o   **Justification:** Simplified menus help users reach the appropriate department quickly and efficiently.
2. **Training and Empowerment of Staff:**
o   **Recommendation:** Provide comprehensive training for call center staff on handling UCC complaints effectively and empathetically.
o   **Justification:** Well-trained staff can resolve issues more efficiently and provide a better customer experience.
3. **Extended Hours and Multichannel Support:**
o   **Recommendation:** Offer extended call center hours and support through multiple channels (e.g., chat, email) to accommodate different user preferences.
o   **Justification:** Extended hours and multichannel support increase accessibility and convenience for users.

D. Examples from International Best Practices:

1. **United States:**
o   **Federal Trade Commission (FTC):** Offers an online complaint submission portal with real-time tracking and automated updates.
2. **European Union:**
o   **European Consumer Centre (ECC):** Provides a centralized complaint platform accessible via web and phone, with multilingual support and clear tracking features.
3. **Australia:**
o   **Telecommunications Industry Ombudsman (TIO):** Features a user-friendly website with an easy complaint registration process and real-time tracking.
4. **Canada:**
o   **Canadian Radio-television and Telecommunications Commission (CRTC):** Provides a comprehensive online complaint system with accessible design and tracking capabilities.

Conclusion

To enhance the accessibility and effectiveness of UCC complaint handling:

1. **Implement a unified and user-friendly complaint management system** across apps, websites, and call centres.
2. **Ensure compliance with accessibility standards** and provide multilingual support.
3. **Streamline the registration process** and offer real-time tracking and automated updates.
4. **Enhance call center operations** with simplified menus, trained staff, and extended support hours.

These measures will help improve consumer satisfaction, ensure timely resolution of complaints, and enhance overall transparency in handling UCC issues.

Q6. What additional modes of complaints registration, preference registration and consents registration through a very easy and quick process can be implemented?

VNO Response:

To enhance the ease and efficiency of registering complaints, preferences, and consents, implementing additional modes and simplifying processes are essential. Here are some recommendations for additional modes of registration and improvements to make the processes quick and user-friendly:

1. Additional Modes of Registration

A. Mobile Applications:

1. **In-App Registration:**
o   **Recommendation:** Develop dedicated mobile apps that allow users to register complaints, preferences, and consents directly from their smartphones.
o   **Justification:** Mobile apps provide convenience and can integrate features like push notifications for updates.
2. **QR Code Scanning:**
o   **Recommendation:** Include QR codes in physical or digital communications that users can scan to quickly access complaint and preference registration forms.
o   **Justification:** QR codes facilitate instant access and simplify the registration process.

B. Voice-Activated Systems:

1. **Voice Assistants:**
o   **Recommendation:** Integrate complaint and preference registration with popular voice assistants like Amazon Alexa, Google Assistant, or Apple Siri.
o   **Justification:** Voice commands offer a hands-free and accessible way for users to manage their preferences and complaints.
2. **Interactive Voice Response (IVR) Systems:**
o   **Recommendation:** Enhance IVR systems to allow users to file complaints and register preferences through voice commands.
o   **Justification:** IVR systems can streamline the process and reduce reliance on manual entry.

C. Social Media Integration:

1. **Social Media Channels:**
o   **Recommendation:** Enable complaint and preference registration through social media platforms like Twitter, Facebook, or Instagram.
o   **Justification:** Social media integration leverages platforms users are already familiar with, making it easier for them to submit their requests.
2. **Social Media Bots:**

o   **Recommendation:** Use chatbots on social media platforms to handle complaint registration, preference updates, and consent management.
o   **Justification:** Chatbots can provide immediate responses and guide users through the registration process.

D. Web-Based Solutions:

1.   **Online Forms and Portals:**
o   **Recommendation:** Create user-friendly web portals with straightforward forms for registering complaints, preferences, and consents.
o   **Justification:** Web forms allow users to submit information from any device with internet access.
2.   **Email and SMS Integration:**
o   **Recommendation:** Implement systems where users can send an email or SMS to a designated address or number to register complaints or update preferences.
o   **Justification:** Email and SMS provide familiar and widely used communication methods for users.

E. In-Person Kiosks:

1.   **Self-Service Kiosks:**
o   **Recommendation:** Set up self-service kiosks in public places such as malls, service centers, or offices where users can easily register complaints and preferences.
o   **Justification:** Kiosks offer a physical location for users who prefer face-to-face interactions.
2.   **Interactive Terminals:**
o   **Recommendation:** Install interactive terminals in high-traffic areas where users can quickly register their details.
o   **Justification:** Interactive terminals facilitate immediate registration and can be used for multiple purposes.

2. Enhancing the Ease and Speed of Registration

A. Simplified Forms and Processes:

1.   **Minimalist Forms:**
o   **Recommendation:** Design forms with the minimal number of fields required, avoiding unnecessary details and making them straightforward to complete.
o   **Justification:** Simplified forms reduce user effort and increase completion rates.
2.   **Pre-Filled Information:**
o   **Recommendation:** Use pre-filled information for returning users based on previous interactions, reducing the need for redundant data entry.
o   **Justification:** Pre-filled forms save time and streamline the registration process.

B. Real-Time Feedback and Assistance:

1.   **Live Chat Support:**
o   **Recommendation:** Provide live chat support on apps and websites to assist users with registration and answer any questions they may have.

o **Justification:** Real-time assistance helps resolve issues quickly and improves user experience.

2. **Automated Guidance:**

o **Recommendation:** Implement automated guidance and tooltips within forms to help users understand what information is needed.

o **Justification:** Automated guidance helps users complete forms accurately and efficiently.

C. Data Integration and Syncing:

1. **Centralized Database:**

o **Recommendation:** Use a centralized database to store and manage all complaints, preferences, and consents, ensuring seamless integration across various platforms.

o **Justification:** A centralized system ensures consistency and accuracy in data management.

2. **Integration with Other Systems:**

o **Recommendation:** Integrate registration systems with CRM and other customer management systems to streamline processes and avoid duplication.

o **Justification:** Integration enhances efficiency and provides a comprehensive view of customer interactions.

D. Accessibility Considerations:

1. **Inclusive Design:**

o **Recommendation:** Design all registration systems with accessibility features such as screen readers, high-contrast modes, and text-to-speech capabilities.

o **Justification:** Inclusive design ensures that all users, including those with disabilities, can access and use the registration systems.

2. **Multilingual Support:**

o **Recommendation:** Provide registration forms and support in multiple languages to cater to diverse user demographics.

o **Justification:** Multilingual support improves accessibility for non-native speakers and ensures broader reach.

Conclusion

To improve the registration of complaints, preferences, and consents, it is essential to:

1. **Implement additional modes** such as mobile apps, voice-activated systems, social media integration, and self-service kiosks.
2. **Enhance ease and speed** by simplifying forms, providing real-time feedback, ensuring data integration, and considering accessibility.
3. **Ensure user-friendly design** across all platforms to facilitate easy and quick registration processes.

By adopting these measures, service providers can offer a more accessible, efficient, and consumer-friendly approach to managing complaints, preferences, and consents.

Q7.   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 effectiveuse 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.

VNO Response:

Comments on Proactive Detection and Management of Spam Messages and Calls

a. Measures for Proactive Detection of Spam and Effective Use of AI-Based Systems

1. Proactive Detection Using Honeypots:

A. Implementation of Honeypots:

1. **Honeypot Deployment:**
o   **Recommendation:** Deploy honeypots in Local Service Areas (LSAs) to capture spam messages and calls. These honeypots should be virtual numbers or email addresses that appear legitimate but are specifically set up to detect spam.
o   **Justification:** Honeypots act as decoys to attract spammers, helping identify patterns and sources of spam.
2. **Honeypot Management:**
o   **Recommendation:** Establish norms for deploying honeypots, including periodic rotation of numbers/addresses and ensuring they are not used for legitimate communication.
o   **Justification:** Regular rotation helps prevent spammers from recognizing and avoiding honeypots, maintaining their effectiveness.

B. Rules and Logics for Honeypot Use:

1. **Data Collection and Analysis:**
o   **Recommendation:** Collect and analyze data from honeypots to identify spam trends, sources, and characteristics. Use this data to refine detection systems.
o   **Justification:** Analyzing honeypot data helps in understanding spam tactics and improving detection algorithms.
2. **Integration with UCC Systems:**
o   **Recommendation:** Integrate honeypot data with Unified Communication and Commerce (UCC) detection systems to enhance spam detection capabilities.

o   **Justification:** Integration ensures that insights gained from honeypots are used to improve overall spam detection and prevention.

2. Effective Use of AI-Based UCC Detection Systems:

A. Training AI Models:

1. **Data Collection:**
o   **Recommendation:** Gather a diverse dataset of spam and non-spam messages and calls to train AI models. This dataset should include examples from honeypots and other sources.
o   **Justification:** A diverse dataset improves the AI model's ability to generalize and accurately detect various types of spam.
2. **Feature Engineering:**
o   **Recommendation:** Identify key features that distinguish spam from legitimate messages and calls, such as frequency of specific keywords, sender behavior patterns, and message metadata.
o   **Justification:** Feature engineering helps in creating more accurate and effective detection models.
3. **Model Training and Validation:**
o   **Recommendation:** Use supervised learning techniques to train AI models, with regular validation and tuning to maintain accuracy. Implement cross-validation to ensure robustness.
o   **Justification:** Regular training and validation ensure that the AI models stay effective as spam tactics evolve.

B. AI Model Deployment and Monitoring:

1. **Continuous Monitoring:**
o   **Recommendation:** Continuously monitor the performance of AI models in real-world scenarios and update them as needed based on new spam patterns and tactics.
o   **Justification:** Ongoing monitoring ensures that AI models remain effective and adapt to changing spam behaviors.
2. **Feedback Loops:**
o   **Recommendation:** Implement feedback loops where users can report false positives and negatives, helping to refine and improve AI models.
o   **Justification:** Feedback from users helps in identifying and correcting model errors, enhancing overall detection accuracy.

b. Proactive Actions to Stop Further Communications and Actions on Senders

1. Stopping Further Communications:

A. Blocking and Filtering:

1. **Automatic Blocking:**
o   **Recommendation:** Implement automatic blocking of identified spam numbers and addresses based on AI detection systems and honeypot data.
o   **Justification:** Automatic blocking prevents further spam communications from known sources.

2. **Dynamic Filtering:**
o   **Recommendation:** Use dynamic filtering rules to adjust blocking criteria based on emerging spam patterns and new threats.
o   **Justification:** Dynamic filtering helps adapt to new spam tactics and maintain effective protection.

B. Alerts and Notifications:

1. **User Alerts:**
o   **Recommendation:** Notify users when spam communications are detected and blocked, providing information about the nature of the spam and any actions taken.
o   **Justification:** User alerts keep consumers informed and increase transparency.
2. **Sender Notifications:**
o   **Recommendation:** Send notifications to known spammers or violators informing them of the blocking action and the reasons behind it.
o   **Justification:** Notifications serve as a deterrent and provide transparency in enforcement actions.

2. Actions on Senders:

A. Enforcement Measures:

1. **Penalties and Fines:**
o   **Recommendation:** Implement a system of penalties and fines for senders identified as frequent violators of spam regulations.
o   **Justification:** Financial penalties serve as a deterrent and encourage compliance with anti-spam regulations.
2. **Legal Action:**
o   **Recommendation:** Pursue legal actions against persistent spammers, including potential lawsuits or regulatory actions, based on evidence gathered from detection systems.
o   **Justification:** Legal actions address severe violations and can have a broader impact on reducing spam.

B. Collaboration and Reporting:

1. **Industry Collaboration:**
o   **Recommendation:** Collaborate with other industry stakeholders, including telecom operators and technology providers, to share information and strategies for combating spam.
o   **Justification:** Industry collaboration enhances collective efforts and improves overall spam detection and prevention.
2. **Reporting Mechanisms:**
o   **Recommendation:** Establish clear reporting mechanisms for users and other stakeholders to report spam incidents and suspicious activities.
o   **Justification:** Effective reporting mechanisms ensure that all spam activities are captured and addressed promptly.
o

Conclusion

To effectively manage spam messages and calls:

1. **Deploy honeypots** in LSAs and integrate their data with UCC detection systems.
2. **Train AI models** using diverse datasets, and continuously monitor and refine them.
3. **Implement automatic blocking** and dynamic filtering to stop further spam communications.
4. **Enforce penalties** and legal actions against persistent spammers.
5. **Collaborate with industry stakeholders** and establish clear reporting mechanisms.

These measures will enhance proactive detection, prevent spam communications, and improve overall effectiveness in managing unsolicited communications.

Q8. 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 oftelemarketers (both RTMs and UTMs) and Principal Entities(Senders), involved in sending UCC and disincentivize them financially including legal actions as per law.

VNO Response:

Comments on Financial Disincentives and Responsibility Assignments

a. Financial Disincentives for Access Providers Against Violations in Respect of RTMs (Registered Telemarketers)

1. Proposed Financial Disincentives:

A. Definition and Scope:

1. **Recommendation:** Clearly define the scope and nature of violations that trigger financial disincentives. This includes breaches such as failing to adhere to regulatory requirements, improper handling of RTM registrations, and failure to enforce compliance with the rules.
   - **Justification:** Clear definitions ensure that access providers are aware of what constitutes a violation and the associated penalties.
2. **Graduated Penalties:**

o **Recommendation:** Implement a graduated penalty system where the financial disincentive increases with the severity and frequency of violations. For example, a tiered penalty structure where minor infractions incur lower fines, while repeated or severe violations lead to higher fines.

o **Justification:** Graduated penalties provide a proportional response to violations and incentivize access providers to improve compliance over time.

B. Implementation and Enforcement:

1. **Regular Audits:**

o **Recommendation:** Conduct regular audits of access providers to ensure compliance with RTM regulations. Use audit results to determine the applicability of financial disincentives.

o **Justification:** Regular audits help maintain ongoing compliance and provide a basis for enforcing penalties.

2. **Transparency in Reporting:**

o **Recommendation:** Ensure transparency in reporting violations and penalties. Provide access providers with clear documentation of infractions and corresponding financial disincentives.

o **Justification:** Transparency helps access providers understand the basis for penalties and encourages them to address compliance issues.

b. Financial Disincentives for Access Providers Against Violations in Respect of UTMs (Unregistered Telemarketers)

1. Proposed Financial Disincentives:

A. Scope of Violations:

1. **Recommendation:** Define violations related to UTMs, such as failing to block or report unregistered telemarketers and inadequate monitoring of UTM activities.

o **Justification:** Clear definitions ensure access providers understand their responsibilities and the consequences of failing to meet them.

2. **Penalty Framework:**

o **Recommendation:** Establish a penalty framework for violations involving UTMs, including fixed penalties for specific infractions and higher fines for repeated or egregious violations.

o **Justification:** A structured penalty framework provides consistency and fairness in enforcing disincentives.

B. Monitoring and Compliance:

1. **Enhanced Monitoring Systems:**

o **Recommendation:** Implement enhanced monitoring systems to track UTM activities and detect non-compliance by access providers. Use these systems to enforce financial disincentives.

o **Justification:** Advanced monitoring systems improve the detection of violations and ensure accurate application of penalties.

2. **Collaboration with Regulatory Bodies:**

- o **Recommendation:** Collaborate with regulatory bodies to share information about UTM violations and ensure coordinated enforcement of financial disincentives.
- o **Justification:** Collaboration enhances the effectiveness of regulatory actions and ensures a unified approach to managing UTMs.

c. Financial Disincentives for Wrong Approval of Headers and Message Templates

1. Proposed Financial Disincentives:

A. Definition and Scope:

1. **Recommendation:** Define the criteria for what constitutes "wrong approval" of headers and message templates, including errors, non-compliance with regulations, or fraudulent approvals.
- o **Justification:** Clear criteria ensure that financial disincentives are applied consistently and fairly.
2. **Penalty Structure:**
- o **Recommendation:** Implement a penalty structure for wrong approvals, including fines for each instance of incorrect approval and higher fines for systemic issues or repeated errors.
- o **Justification:** A structured penalty system provides a clear incentive for accurate and compliant approvals.

B. Enforcement and Verification:

1. **Regular Review Processes:**
- o **Recommendation:** Establish regular review processes to audit header and message template approvals and verify compliance with regulations.
- o **Justification:** Regular reviews help detect and correct issues promptly, reducing the likelihood of wrong approvals.
2. **Transparency and Reporting:**
- o **Recommendation:** Maintain transparency in the approval process and reporting of wrong approvals, ensuring that access providers receive clear documentation of any issues and penalties.
- o **Justification:** Transparency promotes accountability and encourages accurate approvals.

d. Responsibilities and Financial Disincentives for Telemarketers and Principal Entities

1. Assigning Responsibilities:

A. Clear Definition of Roles:

1. **Recommendation:** Define the responsibilities of telemarketers (both RTMs and UTMs) and Principal Entities (Senders) clearly, including compliance with regulations, accurate registration, and adherence to communication standards.
- o **Justification:** Clear role definitions ensure that all parties understand their obligations and the consequences of non-compliance.

2. **Documentation and Reporting:**
o **Recommendation:** Require telemarketers and Principal Entities to maintain detailed documentation of their activities and submit regular compliance reports.
o **Justification:** Documentation and reporting provide a basis for monitoring compliance and addressing violations.

B. Financial Disincentives and Legal Actions:

1. **Penalties for Non-Compliance:**
o **Recommendation:** Implement financial penalties for telemarketers and Principal Entities that fail to comply with regulations, including fines for specific infractions and higher penalties for repeated or severe violations.
o **Justification:** Financial penalties provide a deterrent and encourage compliance with regulations.
2. **Legal Actions:**
o **Recommendation:** Pursue legal actions against telemarketers and Principal Entities involved in significant or repeated violations, including potential lawsuits and regulatory actions.
o **Justification:** Legal actions address severe violations and reinforce the importance of compliance.

C. Incentives for Compliance:

1. **Incentive Programs:**
o **Recommendation:** Consider implementing incentive programs for telemarketers and Principal Entities that demonstrate consistent compliance and adherence to best practices.
o **Justification:** Incentives provide positive reinforcement for compliance and encourage best practices.
2. **Certification and Recognition:**
o **Recommendation:** Provide certification or recognition for telemarketers and Principal Entities that achieve and maintain high standards of compliance.
o **Justification:** Certification and recognition enhance the reputation of compliant entities and motivate others to follow suit.

Conclusion

To address financial disincentives and responsibilities related to UCC management:

1. **Define and implement clear financial disincentives** for access providers, telemarketers, and Principal Entities involved in violations, including RTMs, UTMs, and wrong approvals.
2. **Establish a structured penalty framework** with graduated penalties and regular audits to ensure fair and effective enforcement.
3. **Assign clear responsibilities** to all parties involved and implement both financial disincentives and legal actions to address non-compliance.

By adopting these measures, regulatory bodies can enhance compliance, reduce violations, and improve the overall effectiveness of UCC management.

VNO Response:

Review of Exemptions for Transactional Messages

Question: Whether there is a need to review exemptions accorded to transactional messages and bring them at par with other commercial messages? If yes, please provide justifications. If no, what additional measures are required to discourage misuse of transactional message templates for sending promotional messages?

Review of Exemptions for Transactional Messages

1. Need for Reviewing Exemptions:

A. Current Exemptions and Their Implications:

- **Justification for Review:**
o **Abuse and Misuse:** Transactional messages are intended to provide essential information related to a customer's interactions with a service or product, such as OTPs, transaction confirmations, or account alerts. However, some senders may misuse these exemptions by using transactional message templates to send promotional content.
o **Regulatory Gaps:** Current exemptions may create regulatory gaps, where senders exploit the lack of stringent controls on transactional messages to circumvent restrictions on promotional communications. This undermines the effectiveness of regulations designed to protect consumers from unwanted promotions.

B. Justifications for Bringing Transactional Messages at Par with Other Commercial Messages:

1. **Consumer Protection:**
o **Recommendation:** Align transactional messages with the regulatory framework for other commercial messages to ensure that all communications, regardless of their nature, adhere to strict consent and opt-out requirements.
o **Justification:** By treating all types of communications similarly, consumers are better protected from unwanted messages, regardless of the message's classification.
2. **Consistency and Fairness:**
o **Recommendation:** Apply uniform regulations to all commercial messages, including transactional messages, to ensure consistency in how different types of communications are handled.
o **Justification:** Uniform regulations reduce confusion for consumers and businesses, and ensure fair treatment of all types of commercial communications.
3. **Preventing Misuse:**

o   **Recommendation:** Implement stricter controls on transactional messages to prevent their misuse for promotional purposes, such as requiring explicit consent for all transactional messages and providing clear opt-out mechanisms.

o   **Justification:** Stricter controls reduce the likelihood of senders exploiting transactional message exemptions to deliver promotional content, ensuring that communications are appropriate and consented to.

Additional Measures to Discourage Misuse of Transactional Message Templates

1. Strengthening Definitions and Criteria:

A. Clear Definition of Transactional Messages:

- **Recommendation:** Clearly define what constitutes a transactional message to prevent ambiguity and misuse. Include criteria that differentiate transactional content from promotional content.
- **Justification:** Clear definitions help ensure that messages classified as transactional meet specific criteria and are not used for promotional purposes.

B. Enhanced Monitoring and Compliance:

- **Recommendation:** Implement monitoring systems to detect and prevent misuse of transactional message templates. Regularly review message content and sender practices to ensure compliance.
- **Justification:** Effective monitoring helps identify and address misuse of transactional messages, ensuring adherence to regulations.

2. Consent and Opt-Out Mechanisms:

A. Mandatory Consent for Transactional Messages:

- **Recommendation:** Require explicit consent for all transactional messages, similar to the requirements for promotional messages. Ensure that recipients have clearly opted in to receive these messages.
- **Justification:** Explicit consent ensures that recipients are aware of and agree to receive transactional messages, reducing the risk of misuse.

B. Opt-Out Mechanisms:

- **Recommendation:** Provide clear and easy-to-use opt-out mechanisms for transactional messages, allowing recipients to unsubscribe from future messages if desired.
- **Justification:** Opt-out mechanisms give consumers control over the messages they receive and help prevent the misuse of transactional message templates.

3. Penalties and Enforcement:

A. Financial Penalties for Misuse:

- **Recommendation:** Impose financial penalties on senders who misuse transactional message templates for promotional purposes. Implement a penalty structure based on the severity and frequency of violations.
- **Justification:** Financial penalties serve as a deterrent and encourage compliance with regulations.

B. Regular Audits and Inspections:

- **Recommendation:** Conduct regular audits and inspections of messaging practices to ensure compliance with regulations and identify instances of misuse.
- **Justification:** Regular audits help maintain oversight and enforce compliance, addressing any misuse of transactional message templates.

4. Education and Awareness:

A. Training for Senders:

- **Recommendation:** Provide training and resources to senders and telemarketers on the proper use of transactional message templates and the legal requirements for different types of communications.
- **Justification:** Education helps prevent unintentional misuse and ensures that senders are aware of their responsibilities under the regulations.

B. Consumer Awareness Campaigns:

- **Recommendation:** Run consumer awareness campaigns to inform recipients about their rights regarding transactional and promotional messages, including how to opt out and report misuse.
- **Justification:** Increased consumer awareness empowers individuals to manage their communication preferences and report violations.

Conclusion

1. **Reviewing Exemptions:** There is a need to review the exemptions accorded to transactional messages to ensure they do not undermine consumer protection or allow for misuse. Aligning transactional messages with other commercial communications can enhance fairness and effectiveness in managing unsolicited communications.
2. **Additional Measures:** To discourage misuse, implement clear definitions and criteria, strengthen consent and opt-out mechanisms, enforce penalties, conduct regular audits, and increase education and awareness.

By adopting these measures, regulatory bodies can better manage the use of transactional messages and prevent their misuse for promotional purposes, ultimately improving consumer protection and regulatory effectiveness.

Q.10   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?

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.

VNO Response:

Comments on Strengthening Provisions of Common Code of Practice (CoP) Templates

a. Strengthening the Provisions of Common Code of Practice (CoP) Templates

1. Need for Strengthening CoP Templates:

A. Current Challenges:

- **Lack of Consistency:** Existing CoP templates may lack uniformity in how they address violations and impose financial disincentives, leading to inconsistent enforcement by Access Providers.
- **Inadequate Mechanisms:** Current provisions might not sufficiently cover all scenarios of non-compliance or misuse, limiting the ability of Access Providers to take effective action.

B. Justifications for Strengthening:

1. **Enhanced Compliance Enforcement:**
   - **Recommendation:** Strengthen CoP templates by including standardized processes and clear guidelines for handling violations, imposing financial disincentives, and enforcing regulations.
   - **Justification:** Standardized procedures ensure consistent application of rules and facilitate effective enforcement across different Access Providers.
   -
2. **Clear Protocols for Actions:**
   - **Recommendation:** Define detailed Standard Operating Processes (SOPs) for addressing violations, including steps for investigation, adjudication, and penalties.

o   **Justification:** Clear protocols ensure that violations are handled systematically and fairly, reducing ambiguity and potential disputes.

C. Additional Provisions and Processes for CoPs:

1. **Detailed Violation Categories:**
o   **Recommendation:** Include a comprehensive list of violation categories and associated penalties within the CoP templates. This should cover issues such as misuse of message templates, non-compliance with consent requirements, and failure to adhere to reporting obligations.
o   **Justification:** Detailed categories and penalties help ensure that all types of violations are adequately addressed and that penalties are proportionate to the severity of the breach.
2. **Escalation Procedures:**
o   **Recommendation:** Establish clear escalation procedures for handling severe or repeated violations. This could involve higher-level review boards or regulatory bodies for complex cases.
o   **Justification:** Escalation procedures provide a mechanism for addressing serious breaches and ensure that higher-level expertise is involved in adjudicating complex issues.
3. **Regular Review and Updates:**
o   **Recommendation:** Implement a process for regular review and updating of CoP templates to reflect changes in regulations, emerging trends in misuse, and feedback from stakeholders.
o   **Justification:** Regular updates ensure that CoP templates remain relevant and effective in addressing evolving challenges.

b. Provision for Minimum Security Deposits

1. Justification for Security Deposits:

A. Need for Financial Assurance:

•   **Recommendation:** Introduce a provision for minimum security deposits from entities registering with Access Providers. This deposit would serve as a financial assurance against potential breaches or misuse of regulations.
•   **Justification:** Security deposits provide a financial buffer that can be used to cover costs associated with enforcement actions and penalties, and incentivize compliance by creating a financial stake in adhering to regulations.

B. Provisions for Security Deposit Management:

1. **Deposit Amount and Terms:**
o   **Recommendation:** Specify the minimum amount for security deposits based on the size and risk profile of the entity. Define terms for deposit collection, including the conditions under which deposits are required and the process for replenishment.
o   **Justification:** Setting appropriate deposit amounts ensures that the financial assurance is proportionate to the entity's risk and potential impact on regulatory compliance.
2. **Encashment and Replenishment:**

o   **Recommendation:** Outline clear provisions for the full or partial encashment of security deposits in the event of a breach. Define the process for determining the amount to be encashed, the conditions under which replenishment is required, and the timeline for refunding any unused portion of the deposit.

o   **Justification:** Clear encashment and replenishment provisions ensure transparency and fairness in how deposits are used and managed, providing entities with a clear understanding of their financial obligations and potential consequences.

3. **Compliance Incentives:**

o   **Recommendation:** Offer incentives for entities to maintain full deposits by providing partial refunds or reduced deposit requirements for entities with a history of compliance and positive performance.

o   **Justification:** Incentives encourage entities to adhere to regulations and maintain good compliance records, fostering a culture of accountability.

4. **Dispute Resolution Mechanisms:**

o   **Recommendation:** Include provisions for dispute resolution related to security deposit encashment or replenishment, such as an independent review process or arbitration.

o   **Justification:** Dispute resolution mechanisms provide a fair process for addressing disagreements over deposit-related matters and help maintain trust in the regulatory system.

Conclusion

Strengthening CoP Templates:

- **Enhance** CoP templates with detailed violation categories, clear protocols for handling breaches, and regular review mechanisms to ensure effective enforcement.
- **Standardize** processes to provide consistency in addressing violations and applying financial disincentives.

Security Deposits:

- **Implement** minimum security deposits as financial assurance against breaches, with clear terms for encashment, replenishment, and management.
- **Provide** incentives for compliance and establish dispute resolution mechanisms to ensure fairness and transparency.

By adopting these measures, regulatory bodies can improve the effectiveness of enforcement, enhance compliance, and ensure a fair and transparent system for managing violations and financial disincentives.

Q.11   What effective steps can be taken to control the menace of UCC through tariffs? Please justify your answer.

VNO Response:

Controlling Unsolicited Commercial Communications (UCC) through tariffs can be an effective strategy if implemented thoughtfully. Here are some steps and justifications for using tariffs to address the issue:

Effective Steps to Control UCC Through Tariffs

1. Implement Differential Tariffs for UCC-Related Services

A. Tariff Structure for UCC Communication:

- **Recommendation:** Introduce higher tariffs for sending UCC, such as promotional messages or automated calls. These tariffs could be set at levels that reflect the cost of handling and filtering such communications.
- **Justification:** Higher costs for sending UCC can disincentivize senders from engaging in bulk, unsolicited communications. By increasing the financial burden associated with sending UCC, entities may be less likely to engage in practices that generate revenue through large volumes of unsolicited messages or calls.

B. Lower Tariffs for Opted-In Communications:

- **Recommendation:** Offer lower tariffs for messages or calls sent to recipients who have opted in, such as for verified transactional communications or promotional messages to consenting recipients.
- **Justification:** Reduced costs for opt-in communications incentivize businesses to seek explicit consent from recipients, promoting a more consumer-friendly approach and reducing the prevalence of unsolicited messages.

2. Tariff-based Quality Assurance Mechanisms

A. Premium Services for Compliance:

- **Recommendation:** Provide premium tariff options for senders who adhere to best practices in compliance, such as using validated templates and adhering to consent requirements.
- **Justification:** Premium services for compliant senders can create a financial incentive for businesses to follow regulations and ensure their communications are legitimate, thereby reducing the volume of UCC.

B. Tariff Discounts for Low Complaint Rates:

- **Recommendation:** Offer discounts or rebates on tariffs for entities with low complaint rates and positive compliance records.
- **Justification:** Rewarding entities that maintain low complaint rates encourages adherence to regulations and fosters a culture of responsible communication.

3. Use of Tariffs to Fund UCC Detection and Enforcement

A. Fund Detection Systems:

- **Recommendation:** Allocate a portion of UCC-related tariffs to fund advanced detection systems, such as AI-based filtering and monitoring tools that identify and block UCC.
- **Justification:** Tariffs can generate revenue that supports the development and maintenance of technology to detect and prevent UCC, enhancing overall enforcement capabilities.

B. Support Enforcement Activities:

- **Recommendation:** Use tariff revenue to support regulatory enforcement activities, including investigations, penalties, and consumer education campaigns.
- **Justification:** Financial resources from tariffs can be reinvested into enforcement and consumer protection efforts, ensuring a more robust response to UCC issues.

4. Implement Progressive Tariffs Based on Volume

A. Volume-Based Tariffs:

- **Recommendation:** Establish progressive tariffs that increase with the volume of messages or calls sent. For example, higher rates could apply to bulk messages or calls beyond a certain threshold.
- **Justification:** Progressive tariffs discourage excessive bulk messaging by making it more expensive to send large volumes of unsolicited communications, thereby reducing overall UCC.

B. Cap on Maximum Charges:

- **Recommendation:** Implement a cap on the maximum tariff charges for UCC to prevent undue financial strain on businesses while still discouraging abuse.
- **Justification:** A cap ensures that tariffs are reasonable and do not create financial barriers for legitimate communication while still serving as a deterrent for excessive UCC.

5. Enhanced Transparency and Reporting Requirements

A. Tariff Transparency:

- **Recommendation:** Require senders to disclose tariff rates and any associated costs transparently to recipients, ensuring that consumers are aware of the financial implications of receiving UCC.

- **Justification:** Transparency helps consumers understand the cost structure of UCC and encourages senders to adhere to regulations to avoid financial penalties.

B. Reporting and Auditing:

- **Recommendation:** Implement reporting and auditing mechanisms to monitor tariff compliance and usage, ensuring that entities are billed appropriately and that tariffs are used effectively to control UCC.
- **Justification:** Regular reporting and auditing provide oversight and help identify any issues or abuses related to tariff structures, ensuring that tariffs achieve their intended goals.

Conclusion

Tariffs can be an effective tool to control the menace of UCC when implemented with a strategic approach:

1. **Differential Tariffs:** Higher tariffs for UCC and lower tariffs for opt-in communications can deter unsolicited messaging while promoting consent-based communication.
2. **Quality Assurance Mechanisms:** Premium services and discounts for compliant entities encourage adherence to best practices and reduce UCC volumes.
3. **Funding Detection and Enforcement:** Revenue from UCC tariffs can support advanced detection systems and enforcement activities, enhancing overall effectiveness.
4. **Volume-Based Tariffs:** Progressive tariffs and caps on maximum charges can prevent excessive bulk messaging while maintaining fairness.
5. **Transparency and Reporting:** Ensuring transparency and implementing robust reporting and auditing mechanisms helps maintain tariff effectiveness and compliance.

By integrating these measures, regulatory bodies can use tariffs not only to disincentivize UCC but also to support broader enforcement and consumer protection initiatives.

Q.12   Whether differential tariff for SMS and Voice calls beyond a certain limit should be introduced to disincentivize UCC through UTMs? Please justify.

VNO Response:

Introduction of Differential Tariffs for SMS and Voice Calls Beyond a Certain Limit to Disincentivize UCC

Overview:

Implementing differential tariffs for SMS and voice calls beyond a certain limit could be an effective strategy to disincentivize Unsolicited Commercial Communications (UCC) through Unsolicited Telemarketing Messages (UTMs). The idea is to increase the cost associated with sending large volumes of unsolicited messages or calls, thereby discouraging entities from engaging in such practices.

Justifications for Differential Tariffs:

1. **Financial Deterrence:**

A. Increased Costs for Bulk Messaging:

o **Recommendation:** Introduce higher tariffs for SMS and voice calls that exceed a predefined threshold.
o **Justification:** Higher costs for sending large volumes of messages or calls create a financial disincentive for entities to engage in bulk unsolicited communications. By raising the price for sending UTMs beyond a certain limit, businesses are less likely to exploit mass messaging techniques to reach potential customers unsolicited.

B. Reduced Viability of Bulk Campaigns:

o **Recommendation:** Establish a tiered tariff system where the cost per message or call increases with the volume sent.
o **Justification:** Progressive tariffs make bulk messaging less economically viable, encouraging businesses to seek more targeted and consent-based communication strategies. This can lead to a reduction in the overall volume of UCC.
2. **Encouragement of Opt-In Communication:**

A. Lower Tariffs for Opt-In Communications:

o **Recommendation:** Offer reduced tariffs for messages and calls sent to recipients who have opted in.
o **Justification:** Lower tariffs for opt-in communications provide an incentive for businesses to seek explicit consent from recipients. This encourages a shift towards more consumer-friendly practices and helps to ensure that communications are welcomed rather than unsolicited.
3. **Cost Recovery for Enforcement and Compliance:**

A. Funding for UCC Detection Systems:

o **Recommendation:** Use the revenue from higher tariffs on UCC to fund detection and monitoring systems.
o **Justification:** Additional revenue generated from differential tariffs can be reinvested into advanced technologies and systems for detecting and managing UCC. This includes AI-based systems for filtering and monitoring, which can enhance regulatory enforcement.

B. Supporting Regulatory Actions:

o **Recommendation:** Allocate funds from higher tariffs to support regulatory enforcement activities and consumer protection initiatives.

o **Justification:** Revenue from differential tariffs can be used to support enforcement actions, including investigations into UCC complaints and penalties for non-compliance. This ensures that regulatory bodies have the resources needed to address UCC effectively.

4. **Promoting Fair Market Practices:**

A. Levelling the Playing Field:

o **Recommendation:** Ensure that differential tariffs are applied uniformly to all entities to avoid market distortions.
o **Justification:** Uniform application of tariffs prevents competitive disadvantages for businesses that adhere to regulations and helps maintain a level playing field in the market. This encourages all entities to comply with best practices for consumer communication.

B. Encouraging Best Practices:

o **Recommendation:** Link tariff reductions to adherence to best practices, such as using validated templates and maintaining low complaint rates.
o **Justification:** By providing financial incentives for adherence to best practices, businesses are motivated to follow regulations and adopt responsible communication strategies, further reducing UCC.
o
5. **Consumer Protection:**

A. Enhancing Consumer Control:

o **Recommendation:** Use tariff structures to support consumer protection measures, such as opt-out mechanisms and consent management systems.
o **Justification:** Tariffs can be designed to support systems that give consumers greater control over the communications they receive, ensuring that they have the ability to manage their preferences effectively.

B. Reducing Consumer Complaints:

o **Recommendation:** Implement measures to monitor and address the impact of differential tariffs on consumer complaints.
o **Justification:** Monitoring the effectiveness of differential tariffs in reducing consumer complaints provides insights into their impact and allows for adjustments to be made as needed.

Conclusion:

Introducing differential tariffs for SMS and voice calls beyond a certain limit offers several advantages in disincentivizing UCC through UTMs:

1. **Financial Deterrence:** Higher costs for bulk messaging make it less attractive for entities to engage in unsolicited communications.
2. **Incentivizing Opt-In Practices:** Lower tariffs for opt-in communications encourage businesses to obtain explicit consent from recipients.

3. **Funding Enforcement:** Revenue from differential tariffs can support UCC detection and enforcement efforts.
4. **Fair Market Practices:** Uniform application of tariffs ensures a level playing field and promotes responsible communication practices.
5. **Consumer Protection:** Tariffs can be used to support consumer control and reduce complaints.

Overall, differential tariffs can be a powerful tool in reducing UCC and promoting more consumer-friendly communication practices.

Q.13 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.

VNO Response:

Introducing Differential Tariffs for Voice Calls and SMS

If differential tariffs are to be implemented, setting appropriate thresholds is crucial to ensure effectiveness without unduly burdening legitimate communications. Here's a proposed approach to setting these limits and the rationale behind them:

1. Voice Calls

i. Proposed Limit: 1000 Calls Per Day

Rationale:

1. **Volume Considerations:**
o **Average Business Needs:** Most businesses do not require more than 1000 voice calls per day for legitimate purposes. This threshold balances between normal business operations and the prevention of excessive unsolicited communications.
o **Consumer Protection:** A limit of 1000 calls per day is intended to capture high-volume telemarketers without affecting smaller or less frequent campaigns that businesses might run for legitimate purposes.
2. **Cost Effectiveness:**///////////
o **Operational Feasibility:** Setting the limit at 1000 calls ensures that costs are applied to high-volume, potentially abusive practices while avoiding significant financial strain on businesses engaged in legitimate, low-volume communications.
o **Enforcement and Monitoring:** A clear threshold facilitates easier monitoring and enforcement of the differential tariff system.
3. **Industry Standards:**

- **Comparable Practices:** Similar thresholds are used in other jurisdictions to manage high-volume calling practices. This limit is aimed at distinguishing between normal usage and potential abuse.

2. SMS

ii. Proposed Limit: 5000 Messages Per Day

Rationale:

1. **Volume Considerations:**
- **Business Requirements:** 5000 SMS messages per day is a reasonable limit for high-volume promotional campaigns. This threshold aims to target bulk senders who are likely engaging in unsolicited marketing, while allowing room for legitimate use cases.
- **Consumer Impact:** Limiting the volume helps mitigate the risk of overwhelming consumers with unsolicited messages while not excessively penalizing businesses that have legitimate high-volume needs.
2. **Cost Effectiveness:**
- **Scalability:** The SMS limit is set high enough to cover most legitimate business needs but introduces higher costs for exceeding this volume, thereby discouraging mass unsolicited messaging.
- **Manageable Implementation:** A threshold of 5000 messages per day allows for manageable tariff implementation and monitoring, ensuring that businesses engaged in abusive practices face higher costs.
3. **Industry Standards:**
- **Global Practices:** Other countries with similar regulatory measures use comparable limits to balance between controlling spam and allowing legitimate business communications. This approach aligns with global best practices for managing UCC.

Justification and Implementation Considerations

**1. Consumer Protection and Fairness:

- **Purpose:** Differential tariffs should protect consumers from being inundated with unsolicited communications while allowing businesses to operate within reasonable bounds.
- **Balance:** Setting thresholds prevents excessive financial penalties for smaller, legitimate operations while still targeting high-volume abusers.

**2. Economic Impact:

- **Business Operations:** The proposed limits take into account the typical volume of communications businesses handle, aiming to ensure that costs are imposed primarily on those with high volumes of unsolicited messages or calls.
- **Cost Implications:** Differential tariffs should be set to sufficiently deter abuse without causing undue hardship to businesses engaged in legitimate communications.

**3. Monitoring and Enforcement:

- **Feasibility:** The proposed limits provide clear metrics for monitoring and enforcement. Access Providers can use these thresholds to implement and enforce differential tariffs effectively.
- **Adaptability:** Regular reviews and adjustments to these limits may be necessary based on industry feedback and evolving communication patterns.

**4. Consumer Preferences:

- **Opt-In Trends:** Encouraging opt-in practices through financial disincentives aligns with consumer preference for receiving communications only from entities they have consented to.
- **Transparency:** Clear communication about tariff structures and thresholds helps maintain trust between businesses and consumers.

Conclusion

Setting differential tariffs with thresholds of 1000 voice calls per day and 5000 SMS per day balances the need to disincentivize excessive unsolicited communications while allowing room for legitimate business operations. These thresholds are designed to:

1. **Protect Consumers:** Minimize the impact of UCC on consumers by targeting high-volume abusers.
2. **Support Businesses:** Avoid imposing excessive financial burdens on businesses with legitimate communication needs.
3. **Facilitate Enforcement:** Provide clear metrics for monitoring and implementing tariffs effectively.

Regular assessment and adjustment of these thresholds may be needed to ensure they remain effective and fair as communication practices evolve.

Q.14   If differential tariff is introduced, what could be the tariff beyonda limit for:

iii. Voice calls.

iv. SMS.

Please justify with rationale.

VNO Response:

Proposed Differential Tariffs Beyond Limits for Voice Calls and SMS

Introducing differential tariffs can effectively deter excessive unsolicited communications while ensuring that legitimate communications remain feasible. Below are proposed tariffs for exceeding the specified limits, along with the rationale for these rates:

1. Voice Calls

i. Proposed Tariff Beyond Limit: $0.05 per Call

Rationale:

1. **Economic Deterrent:**
o **Cost-Benefit Analysis:** A tariff of $0.05 per call for volumes exceeding the limit is high enough to act as a deterrent for high-volume unsolicited calls while remaining manageable for businesses that occasionally exceed the limit.
o **Market Comparison:** This rate aligns with or is slightly higher than international benchmarks for similar practices, making it effective without being excessively punitive.
2. **Balance for Legitimate Use:**
o **Operational Feasibility:** For most businesses, this tariff level would be a manageable cost if they occasionally exceed the threshold, ensuring that only consistent abusers face significant financial consequences.
o **Consumer Protection:** By setting a relatively high tariff, it ensures that entities engaging in excessive unsolicited calls face meaningful financial penalties, reducing the incentive for such practices.
3. **Incentive for Compliance:**
o **Encouragement to Adhere:** The cost is set to encourage businesses to stay within the established limits and adopt more targeted communication strategies, thereby promoting better compliance with regulations.

2. SMS

ii. Proposed Tariff Beyond Limit: $0.01 per SMS

Rationale:

1. **Economic Deterrent:**
o **Effective Deterrence:** A tariff of $0.01 per SMS for messages beyond the limit strikes a balance between discouraging excessive messaging and allowing for high-volume but legitimate use cases. This rate is significant enough to dissuade mass unsolicited messaging while being low enough to not overly burden legitimate bulk SMS operations.
o **International Standards:** This rate is competitive with international tariffs, which aim to discourage spam without severely impacting legitimate communication businesses.
2. **Balance for Legitimate Use:**
o **Affordability:** The proposed tariff allows businesses to continue legitimate high-volume SMS campaigns while ensuring that excessive or spammy messages incur additional costs. This helps maintain operational flexibility for businesses that adhere to the rules.
o **Consumer Impact:** Ensures that companies engaging in spam or unsolicited communications face a financial penalty, helping to protect consumers from unwanted messages.

3. **Encouragement for Compliance:**
o **Operational Adjustments:** The cost is set to encourage businesses to manage their SMS volumes effectively and avoid crossing the threshold, thus promoting better adherence to regulations and reducing spam.

General Considerations for Setting Differential Tariffs

**1. Impact on Business Operations:

- **Scalability:** The tariffs should be high enough to deter abusive practices but not so high as to create undue hardship for businesses engaged in legitimate operations.
- **Cost Management:** Businesses should be able to manage their costs and stay within the limits to avoid higher tariffs. This balance ensures fairness and encourages compliance.

**2. Consumer Protection:

- **Deterrence:** Higher tariffs for exceeding limits help protect consumers from excessive unsolicited communications, making it less financially viable for entities to engage in such practices.
- **Transparency:** Clear communication about the tariffs and limits helps businesses understand the consequences of exceeding the thresholds and encourages adherence to the rules.

**3. Enforcement and Monitoring:

- **Practical Implementation:** Tariffs should be set at levels that can be effectively monitored and enforced by Access Providers. This includes having systems in place to track and bill for communications that exceed the established limits.
- **Adaptability:** Regular reviews of the tariff levels and limits may be necessary to adjust for changes in communication practices and technological advancements.

**4. Global Best Practices:

- **Benchmarking:** The proposed tariffs are aligned with international best practices for managing high volumes of communications, ensuring that the measures are effective and comparable to those used in other jurisdictions.

Conclusion

The proposed differential tariffs of $0.05 per voice call and $0.01 per SMS beyond the established limits are designed to:

1. **Discourage Excessive Communication:** Provide a financial deterrent for entities that engage in high volumes of unsolicited calls or messages.
2. **Allow for Legitimate Use:** Ensure that legitimate businesses can operate without undue financial burden while still facing penalties for excessive unsolicited communications.
3. **Protect Consumers:** Reduce the incidence of unsolicited communications, protecting consumers from unwanted messages and calls.

4. **Ensure Effective Enforcement:** Set tariffs at levels that are manageable for enforcement and monitoring by Access Providers.

These tariffs aim to strike a balance between discouraging spam and supporting legitimate communication needs, thereby fostering a more consumer-friendly communication environment.

Q.15   Whether differential tariff should be introduced in a graded manner? If so, please suggest the methodology with justification.

VNO Response:

Introducing Differential Tariffs in a Graded Manner

A graded approach to differential tariffs can be an effective way to manage unsolicited communication without placing undue burden on legitimate communication practices. This method allows for a structured way to apply tariffs based on the volume of communication and the extent of deviation from established limits. Below is a suggested methodology for implementing graded differential tariffs, along with the rationale for each step:

Methodology for Graded Differential Tariffs

**1. Establish Thresholds and Tariff Tiers

i. Voice Calls:

- **Tier 1:** Up to 1,000 calls per day — No additional tariff
- **Tier 2:** 1,001 to 5,000 calls per day — $0.02 per call
- **Tier 3:** 5,001 to 10,000 calls per day — $0.05 per call
- **Tier 4:** Above 10,000 calls per day — $0.10 per call

ii. SMS:

- **Tier 1:** Up to 5,000 messages per day — No additional tariff
- **Tier 2:** 5,001 to 20,000 messages per day — $0.005 per SMS
- **Tier 3:** 20,001 to 50,000 messages per day — $0.01 per SMS
- **Tier 4:** Above 50,000 messages per day — $0.02 per SMS

Justification for the Graded Methodology

**1. Encourages Compliance and Fairness

- **Proportional Penalties:** The graded tariff structure ensures that penalties are proportional to the volume of communication. Businesses that exceed the limit by a small margin face lower additional costs, while those engaging in high-volume unsolicited communications face more substantial financial deterrents.
- **Flexibility:** This approach provides flexibility for legitimate businesses that may occasionally exceed the limits but are not consistently engaging in abusive practices.

2. Supports Legitimate Communications

- **Minimizes Impact:** By providing a tiered system, businesses with occasional high-volume communications are less likely to be unduly penalized. This ensures that legitimate communication needs are not hampered while still addressing excessive unsolicited communications.
- **Encourages Responsible Practices:** Businesses are motivated to stay within the lower tiers to avoid higher costs, promoting responsible communication practices.

3. Facilitates Effective Monitoring and Enforcement

- **Clear Metrics:** The tiered structure provides clear thresholds and associated tariffs, making it easier for Access Providers to monitor and enforce compliance. This clarity helps in managing and tracking communications more effectively.
- **Scalable Enforcement:** The graded system allows for scalable enforcement, where higher tiers involve more rigorous monitoring and penalty application, while lower tiers involve less stringent measures.

4. Aligns with International Best Practices

- **Global Precedents:** Many countries use graduated systems for regulating communication volumes. For example, the European Union's General Data Protection Regulation (GDPR) imposes fines that increase with the severity of non-compliance, and similar graduated approaches are seen in other regions for managing spam and unsolicited communications.
-

5. Adaptability and Review

- **Periodic Reviews:** The graded tariff system should be subject to periodic review to ensure that the thresholds and tariffs remain appropriate as communication practices and technologies evolve.
- **Stakeholder Feedback:** Ongoing feedback from stakeholders can help refine the tiers and tariffs to better meet the objectives of reducing unsolicited communications while supporting legitimate business operations.

Implementation Considerations

1. Communication and Transparency

- **Clear Guidelines:** Access Providers should clearly communicate the thresholds and tariff tiers to all relevant stakeholders, ensuring that businesses understand the financial implications of exceeding the limits.
- **Education and Support:** Provide resources and support to help businesses manage their communication volumes effectively and stay within the established limits.

2. Monitoring and Data Management

- **Robust Systems:** Implement robust monitoring systems to accurately track communication volumes and apply the appropriate tariffs. This may involve advanced analytics and reporting tools.
- **Data Accuracy:** Ensure that data used to determine tariff tiers is accurate and up-to-date to avoid disputes and ensure fair application of the tariffs.

**3. Flexibility and Adjustment

- **Adjustable Limits:** The limits and tariffs should be adjustable based on changing communication patterns and technological advancements. Regular adjustments ensure that the system remains effective and relevant.

Conclusion

A graded differential tariff system is a balanced approach to managing unsolicited communications. By setting clear thresholds and applying tariffs in a tiered manner, it:

1. **Encourages Compliance:** Motivates businesses to adhere to limits and engage in responsible communication practices.
2. **Supports Legitimate Use:** Allows for high-volume communications where necessary while penalizing excessive unsolicited communications.
3. **Facilitates Enforcement:** Provides a clear framework for monitoring and enforcing compliance.
4. **Aligns with Global Practices:** Reflects best practices used internationally for managing spam and unsolicited communications.

This methodology ensures a fair and effective system for reducing unsolicited communications while supporting legitimate business needs. Regular reviews and stakeholder feedback are essential to maintaining its effectiveness and relevance.

****