



Robocall Mitigation Program (Updated)

Purpose

This document describes the robocall mitigation measures implemented by our organization to prevent illegal, unwanted, or spoofed robocalls from originating on our network. These measures are designed to comply with applicable FCC requirements, including participation in the Robocall Mitigation Database (RMD), and to ensure ongoing protection of consumers and downstream carriers.

Current Status

To date, we have not identified any illegal robocall activity originating from our network. We maintain a proactive and continuously improving robocall mitigation framework to ensure that such activity does not occur.

Robocall Mitigation Measures

1. Customer Due Diligence

- We verify the identity, legitimacy, and nature of business of every customer prior to provisioning services.
- Customer onboarding includes review of corporate documentation, authorized signatories, service use cases, and intended call traffic profiles.
- Services are provided only after successful completion of Know Your Customer (KYC) and internal approval processes.

2. Prohibition of Caller ID Spoofing

- Caller ID spoofing is not permitted on our network.
- Only telephone numbers that are assigned or explicitly approved by us may be used as outbound caller IDs.
- Customers are technically restricted from modifying or presenting unauthorized or altered caller IDs.
- Any attempt to use a non-assigned or unauthorized caller ID is automatically blocked by our cloud application platform.





3. Caller ID Validation

- All caller IDs assigned to customers are verified as callable and valid before being enabled for outbound calling.
- We maintain internal records linking caller IDs to specific customers and approved use cases.

4. End-User Only Policy

- Customers must be the end users of the VoIP services provided.
- Resale, re-origination, or sub-assignment of services to third parties is strictly prohibited.

5. Prerecorded and Automated Message Controls

- Prerecorded or artificial voice messages are not permitted unless they clearly identify:
 - The legal name of the entity initiating the call, and
 - A valid telephone number through which that entity can be contacted.
- The identity disclosed in the message must match the customer's verified KYC information.

6. Content Review and Maker-Checker Controls

- Any prerecorded or automated message content must be submitted in advance for review.
- Messages are approved only after verification by our operations team.
- A maker-checker (dual control) process is enforced within our platform before such content can be activated.

7. Traffic Monitoring and Analytics

- We continuously monitor call traffic patterns and Call Detail Records (CDRs).
- Automated and manual reviews are used to detect anomalies such as high-volume bursts, short-duration calls, or complaint-driven indicators of abuse.

8. Abuse Response and Enforcement

- We maintain a dedicated abuse mitigation team responsible for immediate investigation of suspected misuse.
- Upon detection of potential robocall activity, we take prompt corrective action, which may include call blocking, suspension of services, or termination of the customer account.
- We haven't had any incident related to abuse from one of our customers, but we are ready to document incidents and remediation actions for compliance and audit purposes.





9. Customer Relationship and Ongoing Oversight

- We maintain a direct contractual relationship with all customers.
- In addition to telephony services, we provide IT and managed services that allow for periodic site visits, device management, and oversight of phone systems and extensions.
- This close relationship enables early detection of misconfigurations or misuse.

10. Continuous Improvement

- Our robocall mitigation practices are reviewed and updated periodically to address evolving threats, regulatory changes, and industry best practices.
- Employees involved in provisioning, operations, and support receive ongoing training related to robocall prevention and compliance.

Conclusion

Through rigorous customer vetting, technical controls, active monitoring, and rapid enforcement, we are committed to preventing illegal robocalls from originating on our network and to maintaining full compliance with FCC robocall mitigation requirements.

