

Robocall Mitigation Program Description

Overview

The filer is a facilities-based and/or interconnected VoIP service provider that originates voice traffic on behalf of its customers. The filer has not yet implemented the STIR/SHAKEN authentication framework on its network and therefore maintains this robocall mitigation program pursuant to **47 CFR § 64.6305** to ensure that all calls it originates are subject to reasonable steps designed to prevent the origination of illegal robocall traffic.

1. Customer Vetting and Onboarding

The filer implements reasonable customer vetting procedures prior to enabling outbound calling capabilities. These procedures may include, but are not limited to:

- Collection of customer identifying information (legal name, contact information, service address)
- Validation of billing and payment information
- Verification of customer use case for outbound calling
- Review of customer-provided caller ID numbers to ensure appropriate authorization to use such numbers

Customers are prohibited by contract from originating illegal robocalls, spoofed calls, or other unlawful traffic.

2. Traffic Monitoring and Abuse Detection

The filer monitors outbound call traffic for patterns indicative of illegal or abusive robocalling, including but not limited to:

- High-volume or burst calling behavior inconsistent with stated customer use cases
- Repeated short-duration calls
- Abnormal calling patterns across multiple destinations
- Customer complaints or reports from downstream providers

When suspicious activity is detected, the filer takes appropriate action, which may include investigation, rate limiting, temporary suspension, or termination of service.

3. Response to Traceback Requests

The filer commits to responding **fully and within 24 hours** to all traceback requests received from:

- The Federal Communications Commission (FCC)
- Law enforcement agencies
- The Industry Traceback Group (ITG) or its designated traceback consortium

The filer will cooperate in good faith with traceback investigations and will take prompt corrective action when illegal robocall activity is identified.

4. Enforcement and Remediation

If a customer is found to be originating illegal robocalls or otherwise violating applicable laws or the filer's acceptable use policies, the filer will take immediate and appropriate enforcement action, which may include:

- Warning notices
- Suspension or termination of service
- Blocking of outbound calling privileges
- Reporting to upstream providers or appropriate authorities as required

5. Ongoing Compliance and Future Implementation

The filer reviews and updates its robocall mitigation practices as necessary to remain compliant with FCC rules and industry best practices. The filer intends to implement the STIR/SHAKEN authentication framework on its network when operationally and technically feasible and will update its Robocall Mitigation Database filing accordingly upon implementation.

6. Recordkeeping

The filer maintains records related to customer onboarding, traffic monitoring, investigations, and traceback responses as required to demonstrate compliance with **47 CFR § 64.6305**.

Certification

The filer certifies that this robocall mitigation program is implemented and enforced, and that all calls originated on its network are subject to the measures described herein.