

Robocall Mitigation Program Description

1. Overview In compliance with 47 CFR § 64.6305(d)(ii)-(iii), this Robocall Mitigation Program is designed to prevent the origination of illegal robocalls on our network and ensure compliance with the Federal Communications Commission (FCC) regulations. This program outlines the policies, procedures, and mechanisms implemented to detect, prevent, and remediate illegal robocall traffic.

2. Commitment to STIR/SHAKEN Implementation Our organization has fully implemented the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) authentication framework on all IP-enabled portions of our network. This implementation ensures accurate caller ID verification and reduces the likelihood of caller ID spoofing.

For non-IP portions of our network, where full implementation of STIR/SHAKEN is not feasible, we employ the measures described in this program to mitigate illegal robocalls.

3. Measures to Prevent Illegal Robocalls

A. Traffic Monitoring and Analysis

We employ advanced analytics and monitoring tools to:

- Continuously analyze call patterns and traffic behaviors to detect anomalies consistent with illegal robocalling.
- Identify high-volume, short-duration calls and other known robocall traffic signatures.

B. Caller ID Authentication and Validation

For calls originating on our network:

- STIR/SHAKEN is used to validate caller ID authenticity.
- Calls originating from legacy non-IP systems undergo additional scrutiny through our proprietary validation tools.

C. Customer Screening and Vetting

- We enforce strict customer registration and verification processes before granting access to our network.
- We review and monitor customers' calling behaviors to ensure compliance with legal standards.

D. Blocking and Mitigation Protocols

- Proactive call blocking: Calls identified as illegal or suspicious are blocked in real-time.
 - Blacklisting: Known sources of illegal robocalls are added to our internal blacklist.
 - Remediation: Identified violators are subject to immediate action, including service suspension or termination.
-

4. Steps to Respond to Illegal Robocall Traffic

A. Investigation and Verification

Upon detection of potentially illegal robocall traffic:

- We promptly investigate flagged call patterns using both automated tools and manual analysis.
- Verified illegal traffic is escalated for immediate remediation.

B. Notification and Collaboration

- We notify affected downstream providers and, where applicable, law enforcement and regulatory authorities of verified illegal traffic.
- We cooperate with traceback requests initiated by the Industry Traceback Group (ITG) or other authorized entities.

C. Remediation Actions

- Immediate suspension or termination of service for customers found to be originating illegal robocalls.
 - Assistance to affected parties, including regulatory entities, to mitigate further harm.
-

5. Recordkeeping and Reporting We maintain detailed records of:

- Traffic patterns and analysis results for flagged calls.
- Actions taken to block or mitigate illegal robocalls.
- Communications with affected parties and regulatory entities.

These records are preserved for a minimum of one year and made available to the FCC upon request.

6. Certification of Compliance Our organization certifies compliance with all requirements of 47 CFR § 64.6305(d), including:

- Full implementation of STIR/SHAKEN on IP-enabled portions of our network.
 - Adherence to this Robocall Mitigation Program for non-IP traffic.
 - Submission of accurate and timely certifications and supporting information to the Robocall Mitigation Database.
-

7. Contact Information For inquiries regarding this Robocall Mitigation Program, please contact:

Cortel Technologies, LLC.

100 Davidson Avenue, Suite 107

Somerset, NJ 08873

Attn.: Justin Lippolis, EVP & Treasurer

+1-212-627-4200

contact@cortel.com

Signed: Justin Lippolis

Date: 12/12/2024

