

Robocall Mitigation Program Description for STIR/SHAKEN Compliance

Introduction

This document outlines the Robocall Mitigation Program designed to comply with the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) framework and meets the requirements of 47 CFR § 64.6305. This program aims to reduce illegal robocalls, ensure secure and trustworthy caller identification, and comply with all relevant federal regulations.

Robocall Mitigation Measures for Non-IP Networks

- Identify and block high-risk call traffic patterns.
- Monitor call traffic for anomalies indicative of illegal robocall activity.

Call Analytics, Monitoring, and Auditing

- We conduct periodic audits of call traffic and mitigation systems.
- We employ call analytics to identify and mitigate robocall traffic.
- Utilize real-time data analysis to flag and block suspected robocalls.

Call Authentication Policy:

- We require all outbound calls to include a verified caller ID.

Incident Response Plan:

- Investigate reports of non-compliance or illegal robocalls promptly.
- Take corrective action against customers or partners engaged in illegal robocall activities.
- Escalate unresolved incidents to regulatory authorities when necessary.

Customer Education and Support:

- Educate customers about the dangers of illegal robocalls and methods to protect themselves.
- Provide support for reporting and addressing unwanted calls.

Mitigation Practices

- Proactively monitor and address robocall traffic originating from our network.
- Ensure all call authentication policies align with industry standards and FCC guidelines.
- Collaborate with other service providers to enhance overall network security and mitigate illegal robocall activities.