



Robocall Mitigation Program Description

Overview of Robocall Mitigation Program: This document outlines the Robocall Mitigation Program in compliance with the requirements of 47 CFR § 64.6305. The program is designed to prevent the origination, transmission, and facilitation of illegal robocalls and to meet the standards set forth in DA 24-73 (Filing Instructions Public Notice).

Compliance with 47 CFR § 64.6305

1. Voice Service Providers (§ 64.6305(d)(ii)-(iii))

- Implement STIR/SHAKEN authentication on all IP-enabled networks.
- Develop a plan to address non-IP traffic through alternate mechanisms.
- Regularly monitor network traffic to identify and mitigate potential sources of illegal robocalls.
- Maintain records of call authentication results and share relevant data with downstream providers.

2. Gateway Providers (§ 64.6305(e)(ii)-(iii))

- Require upstream foreign providers to certify compliance with robocall mitigation practices.
- Validate all traffic entering the U.S. network to ensure compliance with STIR/SHAKEN or equivalent standards.
- Ensure the secure exchange of call authentication information across all network handoffs.
- Conduct periodic audits of upstream providers and take corrective action as needed.

3. Nongateway Intermediate Providers (§ 64.6305(f)(ii)-(iii))

- Ensure all traffic passed through their network is authenticated per industry standards.
- Cooperate with originating and terminating providers to implement traceback procedures.
- Maintain accurate call detail records and provide these to enforcement agencies upon request.
- Engage in industry best practices to minimize the transmission of illegal robocalls.

Key Elements of the Mitigation Plan

- **Call Authentication:** Providers must implement and maintain call authentication technologies that align with industry standards, such as STIR/SHAKEN.
- **Traceback Cooperation:** Providers must cooperate with traceback requests and facilitate the identification of the source of illegal robocalls.
- **Traffic Monitoring and Filtering:** Providers are required to actively monitor and filter traffic to detect patterns consistent with illegal robocall activity. Suspicious traffic must be flagged and mitigated immediately.
- **Certifications and Audits:** Providers must obtain certifications from upstream or downstream partners confirming adherence to robocall mitigation practices. Routine audits must be conducted to verify compliance.
- **Customer Education and Reporting:** Providers must implement programs to educate customers on identifying and avoiding illegal robocalls. Mechanisms must be in place for customers to report suspicious activity.