

Robocall Mitigation Program Description

1. Introduction

This Robocall Mitigation Program is established in accordance with the requirements set forth under 47 CFR § 64.6305(d)(ii)-(iii). As a voice service provider that has not fully implemented STIR/SHAKEN across its entire network, Caller Technologies is committed to taking reasonable and effective steps to identify, mitigate, and prevent the origination of illegal robocall traffic. This program is designed to uphold industry best practices, comply with all applicable regulations, and actively collaborate with government agencies, law enforcement, and the industry traceback consortium to deter and combat unlawful calling activity.

2. Scope and Application

This program applies to all network segments, interconnection points, and services under Caller Technologies' operational control. It covers call origination, intermediate call handling, and any portion of the call path for which Caller Technologies is responsible. The approach encompasses the use of analytics tools, ongoing monitoring, and a clear escalation process to identify suspicious traffic promptly.

3. Identification and Mitigation of Illegal Robocalls

To meet the requirements of 47 CFR § 64.6305(d)(ii), Caller Technologies has implemented the following specific, reasonable steps to prevent and mitigate the origination of illegal robocall traffic:

a. Call Analytics and Network Monitoring:

Caller Technologies deploys advanced call analytics solutions that review signaling data, call patterns, calling party numbers, call volumes, and other network indicators. Suspicious patterns—such as sudden spikes in call volume from specific numbers, short-duration calls typical of illegal robocall campaigns, and invalid or unassigned caller ID values—are flagged for further investigation.

b. Caller ID Authentication and Verification:

Although Caller Technologies is still in the process of fully implementing STIR/SHAKEN, it uses available partial STIR/SHAKEN implementations and other caller ID authentication methods where feasible. Caller Technologies also incorporates external data sources, such as known bad number lists and industry-defined high-risk number databases, to confirm caller legitimacy where possible.

c. Blocking and Labeling of Suspected Calls:

When Caller Technologies' analytics or authentication checks identify a high probability of illegal robocall traffic, it promptly takes action. This may include blocking the call at the network level or applying labels that warn end-users. Blocking and labeling decisions are informed by Caller Technologies' internal policies, industry best practices, and legal standards.

d. Regular Policy Reviews and Updates:

Caller Technologies reviews and updates its robocall mitigation strategies, tools, and policies at least quarterly to ensure ongoing effectiveness and compliance. This includes staying informed

of new regulatory developments, adopting emerging technologies, and integrating improved analytics techniques.

e. Customer and Industry Education:

Caller Technologies provides clear guidance and educational materials to customers about how to identify scam calls and utilize call-blocking features. It also shares best practices with peer service providers and industry stakeholders to collectively enhance the ecosystem's resilience against illegal robocalls.

4. Cooperation and Information Sharing

To meet the requirements of 47 CFR § 64.6305(d)(iii), Caller Technologies commits to full cooperation and timely responsiveness in traceback and enforcement efforts:

a. Traceback Requests:

Caller Technologies will respond promptly and comprehensively to all traceback requests from the Commission, law enforcement agencies, and the industry traceback consortium. This includes providing accurate and complete call records, routing information, and other relevant data in a secure and timely manner.

b. Point of Contact for Investigations:

Caller Technologies designates a dedicated compliance officer or department as a primary point of contact for all traceback-related inquiries. This ensures a rapid, efficient communication channel and a consistent approach to supporting investigations.

c. Mitigation of Identified Sources:

Upon receiving notification or identification of a suspected source of illegal robocalls, Caller Technologies will immediately investigate and take appropriate action. Actions may include suspending or terminating accounts responsible for initiating illegal traffic, implementing targeted blocks, and reinforcing authentication measures. Caller Technologies also monitors these sources for any future violations to prevent recurrences.

d. Data Integrity and Privacy Compliance:

While cooperating with traceback requests, Caller Technologies remains committed to protecting the privacy and security of customer information. All disclosures are handled in strict accordance with applicable privacy laws and regulations.

5. Ongoing Improvement and Accountability

Caller Technologies maintains internal accountability through regular audits of its mitigation measures, documented processes, and compliance logs. It tracks performance against key metrics such as the number of identified illegal call campaigns, the speed and effectiveness of responses, and the outcomes of traceback activities. These metrics inform continuous improvement efforts and ensure that the program remains effective, transparent, and fully aligned with regulatory expectations.

6. Conclusion

Through this Robocall Mitigation Program, Caller Technologies affirms its commitment to actively deterring and mitigating illegal robocall traffic. By employing robust analytics, caller ID verification measures, proactive blocking strategies, and full cooperation with traceback investigations, Caller Technologies strives to uphold the integrity of its network and protect its customers from unlawful calling activities in accordance with 47 CFR § 64.6305(d)(ii)-(iii).