

Robocall Mitigation Plan

Business Information

Secure Voice Corp.
30 N. Lincoln Street
Batavia, IL 60510

Contact Information

Brenda Smith
Operations Supervisor
630-301-1132
brenda.smith@securevoicecorp.com

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider" procedures;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

Secure Voice Corp. ("SVC") is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network. SVC is a "pure reseller" intermediate carrier that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, SVC has been exempted from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as SVC now file RMPs. This document delineates SVC's RMP. Because SVC does not have access to the necessary infrastructure, it relies, to some extent, on its upstream carriers to assist in robocall mitigation. As delineated herein, SVC works closely with its upstream provider to carry out the required mitigation functions.

Know Your Customer ("KYC")

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with SVC in which we transmit calls based on behalf of the subscriber.

SVC's KYC program involves obtaining specific information when a subscriber signs up for service. This process includes collecting such information such as:

- name;
- phone number;
- FRN;
- FCC Filer ID;
- physical business location;
- contact person(s); and
- nature of the subscriber's business.

Know Your Upstream Provider

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59*, and Third Notice of Inquiry in CG Docket 17-59 (Rel. May 19, 2023) ¶¶ 49-51,

SVC uses procedures similar to those delineated above in the KYC regarding knowing its upstream carriers. While SVC's contracts with its upstream providers do not contain any provisions regarding robocall mitigation, SVC has received assurances from them that they will cooperate with SVC on robocall mitigation, traceback requests, and will comply with all the FCC's robocall mitigation rules.

Analytics for Monitoring Traffic

SVC works with its upstream provider to identify behaviors which indicate illegal call activity. Examples of calling patterns monitored:

- anomalies in cost generated by calls from a single customer;
- multiple overlapping calls on the same account is a risk of not having a single subscriber using the service;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level); and
- anomalies in call duration distribution (most calls having similar duration is not representative for residential service usage).

Investigate Suspicious Activity

When traffic analysis indicates the presence of potential illegal robocalling, SVC works with its upstream provider to follow defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

Because SVC does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in deploying SVC's analytics.

SVC follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, SVC will devote sufficient resources to provide prompt and complete resources to traceback requests. SVC works with its upstream providers to investigate suspicious activity found by their monitoring systems or reported to SVC by subscribers or third parties.

Blocking

SVC will implement Do Not Originate requests it receives from ITG. SVC has mechanisms to automatically block suspicious calls using internal analytics. If SVC and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, SVC will take appropriate action which may include suspending or terminating the subscriber's use of SVC's service. SVC will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including state attorney generals' offices), as well as the FCC, or ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. SVC will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, SVC will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Brenda Smith

I, Brenda Smith, Operations Supervisor of Secure Voice Corp. ("SVC"), do hereby certify, under penalty of perjury, the following:

- (1) SVC, by virtue of its status as a "pure reseller" does not have access to the necessary infrastructure to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.
- (2) SVC's Business name and primary address are as follows:

Secure Voice Corp.
30 N. Lincoln Street
Batavia, IL 60510

- (3) SVC has no other business names in use.
- (4) SVC has not previously used any other business name. High Wire Networks Inc. is 100% owner of SVC. SVC has no affiliates or subsidiaries.
- (5) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (6) SVC's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (7) SVC has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (8) SVC is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (9) SVC is not required to, and does not have, an operating company number.

Brenda Smith

Brenda Smith