

Robocall Mitigation Plan

Business Information

Satcom Direct, Inc. ("Satcom")
1050 Satcom Lane Melbourne, FL 32940

Contact Information

Jeffrey Keller
VP of Network Services and Engineering
Engineering & Operations Department
321-777-3000
jkeller@satcomdirect.com

Overview

Pursuant to paragraphs 69-72 of the Federal Communications Commission's ("FCC," or "Commission") *Call Authentication Trust Anchor*, Sixth Report & Order and Further Notice of Proposed Rulemaking ("6th Report & Order") in WC Docket No. 17-97, FCC 23-18 (rel. March 17, 2023) and 47 C.F.R. § 64.6304(d), Satcom, which is a satellite operator and a domestic small voice provider, has an indefinite extension from the requirement to be STIR/SHAKEN compliant

The 6th Report & Order also states 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;
- 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

Satcom is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. Satcom is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, Satcom was previously exempt from the FCC's STIR/SHAKEN rules. The 6th Report & Order requires that pure resellers such as Satcom now file RMPs. This document delineates Satcom's RMP. Because Satcom does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated herein, Satcom 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 that subscriber. A subscriber is an entity that has a business

relationship with Satcom in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Satcom's KYC program involves obtaining specific subscriber information when payment is made for services. This process includes collecting such information such as:

- physical business location;
- contact person(s);
- nature of the customer's business.

In addition to that, we utilize Descartes screening services and will be utilizing credit checks.

We procure Direct Inward Dialing (DIDs) numbers through Voxbeam for our Global One Number (GON) and AeroV services.

The DIDs allocated to GON are used for inbound calls only. These numbers are assigned to a customer to allow them to contact their aircraft using a local telephone number vs. a costly international call. Any inbound call would have already been verified by the upstream carrier. Once the call reaches us, our PBX answers the call and waits for the end user to make a predefined selection (setup by Satcom), depending on the selection the call would either be routed outbound over our copper circuits (exempt from STIR/SHAKEN) to a specific satellite phone number or, in less frequent cases, it would be routed internally to our AeroV (VoIP) service never leaving Satcom's infrastructure. Our customers are not able to use these numbers to place outbound calls.

Our AeroV service allows customers to use DIDs as SIP/IAX clients for both inbound and outbound calls. However, strict controls are in place; customers must use the assigned unique password, and their device must be registered on Satcom's network (whitelisted IP range) to make or receive calls. Customer identity is verified based on the registered IP. Manipulation of caller ID or anonymous calling for originating VoIP traffic is prohibited.

The risk of our GON/AeroV DIDs being used for robocalling is next to zero.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls* and *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, FCC 23-37, (rel. May 19, 2023) ¶¶ 49-51, Satcom provides the following information concerning its upstream voice service carrier.

Satcom has one upstream provider from which it receives voice traffic:

Voxbeam Telecommunications Inc. ("Voxbeam")
6314 Kingspointe Pkwy
Suite 1
Orlando, FL 32819
Steve Kay
clec@voxbeam.com

Satcom has a master service agreement with Voxbeam and has received assurances in writing from Voxbeam officials it has, and will continue to, sign calls transmitted to Satcom, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic

to Satcom. Satcom and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

Satcom maintains an AUP that subscribers must agree to before being permitted to use Satcom's network. Among other things, the AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law;
- violating applicable industry accepted guidelines; and
- using Satcom's service to engage in or in connection with fraudulent activities.

Satcom's contractual terms with subscribers specify that Satcom may take action up to suspension or termination of service for violation of the AUP.

Mitigation During Service

We do not allow caller id manipulation or anonymous calling; the caller id must match the DID allocated to the subscriber. We use internal tools to detect unusual calling patterns with automated call blocking if calls meet specific criteria.

Analytics for Monitoring Traffic

Satcom 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 likely illegal robocalling, Satcom 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 Satcom does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in Satcom's analytics.

Satcom follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Satcom will devote sufficient resources to provide prompt and complete resources to traceback requests.

Satcom works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to Satcom by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Satcom contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream provider to block their use of the platform.

For all new and renegotiated Satcom contracts governing the transport of voice calls, Satcom will endeavor to contractually require Satcom's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Satcom automatically blocks calls from a subscriber who has made more than 10 calls within a 15-minutes interval. Satcom will implement Do Not Originate requests it receives from the ITG. Satcom's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If Satcom and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, Satcom will take appropriate action which may include suspending or terminating the subscriber's use of Satcom's service. Satcom will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorney general's office), as well as the FCC, and/or the 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. Satcom 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, Satcom 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 Jeffrey Keller

I, Jeffrey Keller, VP of Network Services and Engineering of Satcom, do hereby certify, under penalty of perjury, the following:

- (1) Satcom, 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) Satcom 's Business name and primary address are as follows:

Satcom Direct, Inc.
1050 Satcom Way, Melbourne FL 32940
- (3) Satcom has no other business names in use.
- (4) Satcom has not previously used any other business name.
- (5) The following entity owns more than 10% of Satcom James W. Jensen Living Trust Dated July 31, 2002.
- (6) The following persons are Satcom's directors: James W. Jensen
- (7) None of the persons/entities in items 5 – 6 above have had their licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (8) 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.
- (9) Satcom's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (10) Satcom has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (11) Satcom is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

Jeffrey T Keller
Jeffrey T Keller (Feb 28, 2024 11:12 EST)

Jeffrey Keller
VP of Network Services & Engineering
Dated: February 28, 2024