

Robocall Mitigation Plan

Business Information

Tresta, Inc.
1950 Commonwealth Lane
Suite A
Tallahassee, FL 32303

Contact Information

Jaclyn Gonzalez
CEO
305-978-3521
jackie.gonzalez@tresta.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, outlines "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;
- ownership information;
- 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

Tresta, Inc. ("Tresta") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. Because Tresta lacks control of the infrastructure necessary to implement STIR/SHAKEN, it is not required to be STIR/SHAKEN compliant. In compliance with the R&O, Tresta submits this RMP and certification.

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 Tresta in which we transmit, originate, and/or terminate calls on behalf of the subscriber.

Tresta'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 collecting the listed information, Tresta uses third-party fraud detection software to verify identities and conduct mobile phone number and email verification steps for new customers.

Acceptable Use Policy ("AUP")

Tresta maintains an AUP that subscribers must agree to before being permitted to use Tresta's network. The AUP prohibits is here: tresta.com/legal/terms-of-use

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

Know Your Upstream Providers

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, Tresta provides the following information concerning its upstream voice service carrier.

Bandwidth Inc.
900 Main Campus Drive
Raleigh NC 27606
Stephen Thayer
voicesecurity@bandwidth.com

Tresta's service agreement with its upstream provider contains no language concerning robocall mitigation. But Tresta and its upstream provider have agreed to work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests. Tresta's upstream provider is listed as STIR/SHAKEN compliant in the Robocall Mitigation Database.

Monitoring With Analytics

Tresta works with its upstream provider to detect a calling pattern consistent with illegal robocalls. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network. Our outbound calling feature only works from our mobile app, which uses mobile bridging to connect calls. An individual person has to manually place each call one by one, which enables seamless monitoring.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Tresta follows the 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;
- verifying that the call originating path is valid; and

- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

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

Blocking

Tresta will implement Do Not Originate requests it receives from the ITG. Tresta works with its upstream carrier to block suspicious calls. If Tresta and its upstream carrier identify suspected robocalling patterns that are confirmed with further investigation, Tresta will take appropriate action which may include suspending or terminating the subscriber's use of Tresta's network. Tresta will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), as well as the FCC and the ITG, as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. TRESTA 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, Tresta 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 Jaclyn Gonzalez

I, Jaclyn Gonzalez, CEO of Tresta, Inc. ("Tresta") do hereby certify, under penalty of perjury, the following:

- a. Tresta is not required to implement STIR/SHAKEN, due to its lack of control over the necessary infrastructure.
- b. Tresta's business name and primary address are as follows:

Tresta, Inc.
1950 Commonwealth Lane
Suite A
Tallahassee, FL 32303

- c. Tresta has two d/b/a's: (1) PATLive, and (2) Hosted Numbers.
- d. Outside of the d/b/a's listed above, Tresta has not previously used any other business names.
- e. 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.
- f. The individuals with 10% or more ownership in the company are: Austin Davidson, Glen Davidson, Sharyn Davidson, Benson Davidson, Tanner Davidson, Kathryn Davidson, and Jaclyn Gonzalez.
- g. Tresta's role in the call chain is that of a voice service provider with no STIR/SHAKEN implementation obligation.
- h. Tresta is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. Tresta has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. Tresta is not required to, and does not have, an Operator Code Number.


Jaclyn Gonzalez