

Robocall Mitigation Plan

Business Information

Reliable PBX Corp ("Reliable PBX")
20 Industrial Ave
Upper Saddle River, New Jersey 07458

Contact Information

Aber Weiss
CEO
8557353600
aber@reliablepbx.com

Overview

In the Commission's recent release, *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd. 2573 (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";
- 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

Reliable PBX is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network.

As certified in the FCC's Robocall Mitigation Database, Reliable PBX has fully implemented STIR/SHAKEN. In compliance with the R&O, Reliable PBX 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 Reliable PBX in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Reliable PBX'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.

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, 38 FCC Rcd 5404 (2023), at ¶¶ 49-51, Reliable PBX provides the following information concerning its upstream voice service carriers.

Reliable PBX has three upstream providers from which it receives voice traffic:

1. Bandwidth Inc
900 Main Campus Drive
Suite 100
Raleigh NC 27606
Stephen Thayer
voicesecurity@bandwidth.com
2. Inteliquent, Inc. DBA Onvoy, Sinch ("Inteliquent")
550 W. Adams St.
Suite 900
Chicago IL 60661
Stacy Graham
Director, Assurance & Trust Services
stacy.graham@sinch.com
217-862-1953
3. Telnyx, LLC
600 Congress Ave
14th Floor
Austin TX 78701
Olive Morris
regulatory@telnyx.com
312 270 8153

Reliable PBX has master service agreements with its upstream providers and has received assurances in writing from their officials that they have, and will continue to, sign calls transmitted to Reliable PBX, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Reliable PBX. Reliable PBX and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

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

- making illegal robocalls;
- 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 Reliable PBX's service to engage in or in connection with fraudulent activities.
- Reliable PBX's contractual terms with subscribers specify that Reliable PBX may take action up to suspension or termination of service for violation of the AUP.

Mitigation During Service

Reliable PBX's subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to that individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting). These features are:

- VoIP-originated calls are signed with subscriber caller ID; and
- requiring authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Analytics for Monitoring Traffic

Reliable PBX works to detect a calling pattern consistent with illegal robocalls. Examples of calling patterns monitored are:

- 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).

If such patterns are detected, we will identify the party who is using our network to originate those calls and will take appropriate action. 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.

No third-party vendors are involved in deploying Reliable PBX's analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Reliable PBX's risk prevention team is alerted, which 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;
- investigating if any system issue generates the strange behavior;
- 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.

Reliable PBX follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Reliable PBX will devote sufficient resources to provide prompt and complete resources to traceback requests. Reliable PBX commits to responding to traceback requests fully within 24 hours.

Blocking

Reliable PBX will promptly respond to Do Not Originate requests it receives from ITG. Reliable PBX has mechanisms to automatically block suspicious calls using internal analytics. If Reliable PBX's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Reliable PBX will take appropriate action which may include suspending or terminating the subscriber's use of Reliable PBX's network. Reliable PBX will cooperate with investigative bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), to the FCC, and/or ITG; as well as documenting requests and actions taken in response thereto.

Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Reliable PBX will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapts to this ever-changing issue.

In the event of any material change to this plan, Reliable PBX 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 Aber Weiss

I, Aber Weiss, CEO of Reliable PBX, do hereby certify, under penalty of perjury, the following:

- (1) Reliable PBX has fully implemented STIR/SHAKEN in the IP portions of its network.
- (1) Reliable PBX's Business name and primary address are as follows:

Reliable PBX Corp
20 Industrial Ave
Upper Saddle River, New Jersey 07458
- (2) Reliable PBX has no other business names in use.
- (3) Reliable PBX has not previously used any other business name.
- (4) 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.
- (5) The following person is the owner and director of Reliable PBX: Aber Weiss. He has not had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) 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.
- (7) Reliable PBX's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (8) Reliable PBX has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) Reliable PBX is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (10) Reliable PBX's Operating Company Number is 919K.

Aber Weiss
Aber Weiss