

Robocall Mitigation Plan

Business Information

WWT Inc., d/b/a VoIP Networks
1951 Old Cuthbert Road, Suite 206
Cherry Hill, NJ 08034

Contact Information

Robert Fusco
SVP
856.795.4500
rob.fusco@voipnetworks.com

Overview

In the Commission's recent 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"), even those that are fully STIR/SHAKEN compliant 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;
- 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

WWT Inc. ("WWT") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. WWT has fully implemented STIR/SHAKEN in the IP portion of its network. In compliance with the R&O, WWT submits this RMP and certification.

Know Your Customer

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

New Subscribers

All new subscribers go through identity verification protocols. These include but are not limited to: name, address, email address, point of contact, nature of subscriber's business and contact phone number.

These identity markers are validated for accuracy. All new subscriber activity is monitored as further explained below.

Existing Subscribers

WWT requires updates of subscribers' information on all their orders. Each order's identity markers are verified again to ensure the account is not compromised and is being used for its intended purpose.

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, WWT provides the following information concerning its upstream voice carriers.

WWT receives voice traffic from two upstream providers:

- 1) Bandwidth Inc. ("Bandwidth")
900 Main Campus Drive
Suite 100
Raleigh NC 27606
Stephen Thayer, Senior Fraud Manager
Email: voicesecurity@bandwidth.com
Tel.: 919-704-3069
- 2) Inteliquent, Inc. DBA Onvoy, Sinch ("Inteliquent")
550 W. Adams St.
Suite 900
Chicago IL 60661
Stacy Graham, Director, Assurance & Trust Services
Email: stacy.graham@sinch.com
Tel.: 217-862-1953

According to the Robocall Mitigation Database, Bandwidth and Inteliquent are fully STIR/SHAKEN compliant. WWT 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

WWT maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use WWT's network. Among other things, this AUP prohibits:

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

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

Telephone Number Authorization

A Telephone Number ("TN")- based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by WWT and/or obtained by WWT from one of WWT's underlying carriers for use by the subscriber. In most cases, WWT directly manages the TNs used by its subscribers. WWT tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of WWT's assignment of the TN to its subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by WWT, then TN validation is necessary. If a subscriber can provide WWT with a valid Letter of Authorization (LOA) and Customer Service Record (CSR) that subscriber is the authorized user of such TNs, WWT will attest calls originated with these TNs.

Analytics for Monitoring Traffic

WWT works with its upstream carriers to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. If WWT detects a calling pattern consistent with illegal robocalls, we will identify the party and take appropriate action. 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 system.

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

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, WWT's risk prevention team is alerted, and 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 particular use case and validate that the activity belongs to that subscriber.

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

WWT will investigate suspicious activity reported to us by subscribers or third parties or underlying carriers. The investigation could potentially result in opening a traceback request or with WWT

contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform.

For all new and renegotiated WWT contracts governing the transport of voice calls, WWT will work to contractually require its subscribers to cooperate in traceback investigations.

Blocking

WWT will implement Do Not Originate requests it receives from the ITG. If WWT's and/or WWT's underlying carriers identify suspected robocalling patterns that are confirmed with further investigation, WWT will take appropriate action which may include suspending or terminating the subscriber's use of WWT's network. WWT will cooperate with Investigative Bodies, including state attorneys general offices, the FCC, and the ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

WWT 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, WWT 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 Robert Fusco

I, Robert Fusco, SVP WWT Inc. ("WWT") do hereby certify, under penalty of perjury, the following:

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

WWT Inc.
1951 Old Cuthbert Road, Suite 206
Cherry Hill, NJ 08034

- (3) WWT has an additional business name, VoIP Networks.
- (4) WWT has not previously used any other business name.
- (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) WWT's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (7) WWT has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (8) WWT is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (9) WWT's Operator Code Number is 053K.

Robert Fusco

Robert Fusco