



MEMORANDUM

TO: FCC, Bandwidth.com
FROM: Nick Lincoln, Operations Manager
DATE: 02/21/2024
RE: **Robocall Mitigation Plan**

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";
- 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

Server At Work LLC ("SAW.IT") is an MSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. As certified in the FCC's Robocall Mitigation Database, Server At Work LLC has fully implemented STIR/SHAKEN. In compliance with the R&O, Server At Work submits this RMP and certification.

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, Server At Work LLC provides the following information concerning its upstream voice service carriers:

Bandwidth.com
900 Main Campus Drive
Suite 100
Raleigh NC 27606
Stephen Thayer



(855) 864-7776

voicesecurity@bandwidth.com

Server At Work LLC follows procedures to ensure that it knows the identities of all its upstream carriers from which it accepts traffic. To the extent that Server At Work LLC were to receive information from law enforcement or other sources that a customer is engaged in illegal robocalling, our policy is to cooperate fully, including providing the identity of any suspected illegal robocaller, pursuant to a legal service or process. While Server At Work LLC's agreements with its upstream providers contain no provisions specific to robocall mitigation, Server At Work LLC has received assurances from them that they have, and will continue to, sign calls submitted to Server At Work LLC, and will abide by the FCC's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to you.

Know Your Customers

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 Server At Work LLC in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

New Subscribers

Server At Work, LLC's onboarding process 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); and
- nature of the customer's business.

Also, all new subscribers go through identity verification protocols. Server At Work LLC rate limits the number of calls per second that can be initiated. All Caller ID's must match customer records and cannot be changed.

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 Server At Work LLC and/or obtained by Server At Work LLC from one of Server At Work LLC's underlying carriers for use by the subscriber. In most cases, Server At Work LLC directly manages the TNs used by its subscribers. Server At Work LLC tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Server At Work LLC'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 Server At Work LLC, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, Server At Work LLC will attest calls originated with these TNs.



When originating a call, Server At Work LLC checks the calling party number against Server At Work LLC's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

During Service

All 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 only after number validation via SMS; and
- Requiring authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our 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 particular use case and validate that the activity belongs to that subscriber.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. Server At Work LLC 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, Server At Work LLC 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.

Regards,

A handwritten signature in black ink, appearing to read 'Nick Lincoln', is positioned below the 'Regards,' text.

Nick Lincoln, Operations Manager
Server At Work, LLC