

Robocall Mitigation Plan

Business Information

Autus Technology, LLC d/b/a Loop Communications
21515 Baltic Dr
Cornelius, NC 28031

Contact Information

Amanda Proffitt
COO
7047545000 ext. 5009
compliance@loopcommunications.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") 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 an 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 an 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

Autus Technology, LLC d/b/a Loop Communications ("Loop Communications") is dedicated to stopping illegal calls from traversing its network and monitoring the calls coming into the network. As certified in the FCC's Robocall Mitigation Database, Loop Communications has fully implemented STIR/SHAKEN. In compliance with the R&O, Loop Communications submits this RMP and certification.

Know Your Customer ("KYC")

To ensure network integrity and compliance with regulatory standards, we implement strict KYC practices, payment controls, and Caller ID restrictions.

1. **Customer Identification & Onboarding.** Potential clients must undergo a thorough identification process before subscribing to our services. We require the following verification details:
 - a. The official legal name of the entity.
 - b. Full physical addresses for all business locations.

- c. Authorized contact personnel designated for each operational location.
- d. Verified physical location addresses are strictly required to properly configure E911 services.

2. Payment & Billing Restrictions

We mitigate financial and operational risk through a controlled, structured billing model:

- a. Services are billed strictly on a monthly basis.
- b. We do not offer or support services on an auto-refill basis, ensuring all transactions are reviewed and processed within standard monthly cycles.

3. Caller ID & Network Limitations

To prevent spoofing and ensure fraudulent traffic does not pass through our infrastructure, we enforce strict limitations on Caller IDs. We only allow Caller IDs that match verified, known Direct Inward Dialing (DID) numbers provisioned on our network. Any traffic attempting to utilize an unverified or external Caller ID is restricted.

Our customer base consists of business entities who originate calls related to their line of work and do not use automated calling technologies. In addition, our end users have access to block callers via a feature code to prevent unwanted calls that may reach them despite traveling through our compliant upstream carriers.

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, Loop Communications provides the following information concerning its upstream voice service carriers.

Loop Communications has three upstream providers from which it receives voice traffic:

1. Telnyx, LLC

600 Congress Ave
14th Floor
Austin TX 78701
Olive Morris
312 270 8153
regulatory@telnyx.com

2. Bandwidth Inc.

2230 Bandmate Way
Raleigh, North Carolina 27607
Stephen Thayer
voicesecurity@bandwidth.com

3. Voyant Communications, LLC

1 North Wacker Dr
Suite 2500
Chicago IL 60606
Stacy Graham
2178621953
stacy.graham@sinch.com

Loop Communications has master service agreements with its upstream providers, who have agreed to diligently collaborate with Loop Communications to mitigate all illegal robocalls, including traceback investigations.

Acceptable Use Policy ("AUP")

Loop Communications maintains an AUP as part of its Terms of Service that subscribers must agree to before being permitted to use its software and services. Among other things, the AUP prohibits:

- using our service for any unlawful purposes whatsoever;
- using the service or the device in any way that is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, or invasive of another's privacy; or
- reselling the service.

Analytics for Monitoring Traffic

Loop Communications works to detect a calling pattern consistent with illegal robocalls. If such a call is detected, we work to identify the party who is using our network to originate those calls and 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.

Our established analytical procedures include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity;
- investigating if any system issue generates the unusual 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.

No third-party vendors are involved in deploying Loop Communications' analytics.

Investigate Suspicious Activity

When suspicious activity or potentially illegal robocalling is flagged, our team initiates a multi-layered incident response protocol:

1. **Immediate Log Analysis** (Phase 1: Detection). We conduct an immediate, comprehensive review of all log files across the necessary servers to trace the source, volume, and patterns of the suspicious traffic.

2. **Access Containment** (Phase 2: Mitigation). To protect network integrity, we block access and restrict traffic from the compromised or suspicious sources as an immediate safeguarding measure.
3. **Course Determination** (Phase 3: Resolution). We evaluate the findings to determine and execute the most effective long-term mitigation course, which may include permanent blocking, upstream provider notification, or traceback collaboration.

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

Blocking

We are fully committed to compliance with Industry Traceback Group (ITG) standards and have established protocols to address "Do Not Originate" (DNO) requests. Specifically, our mechanism includes the following actions:

1. **Timely Implementation:** We process and implement all DNO requests received from the ITG in a timely fashion, strictly adhering to ITG best practices.
2. **Industry Cooperation:** We actively cooperate with all necessary parties, upstream carriers, and regulatory bodies to ensure the integrity of the request is maintained.
3. **Enforcement & Mitigation:** We follow through with all appropriate enforcement actions. This includes, but is not limited to, immediate investigation, mitigation of unauthorized traffic, and up to terminating the user's access and use of our systems for non-compliance.

If Loop Communications' monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Loop Communications will take appropriate action which may include suspending or terminating the subscriber's use of Loop Communications' network. Loop Communications 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. Loop Communications will respond to traceback requests within 24 hours.

Plan Updates

This plan, along with industry's best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Loop Communications will monitor industry's 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, Loop Communications will republish it to employees, consultants and contractors and file an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Amanda Proffitt

I, Amanda Proffitt, COO of Autus Technology, LLC d/b/a Loop Communications ("Loop Communications"), do hereby certify, under penalty of perjury, the following:

(1) Loop Communications has fully implemented STIR/SHAKEN in the IP portions of its network.

(1) Loop Communications' business name and primary address are as follows:

Autus Technology, LLC d/b/a Loop Communications
21515 Baltic Dr
Cornelius, NC 28031

(2) Autus Technology, LLC operates under the business name Loop Communications.

(3) Loop Communications 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) Loop Communications has the following principals: Brian Tolleson, James McKinney, and Amanda Proffitt. Neither of them has had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.

(6) Loop Communications has no parent companies, subsidiaries, or affiliates.

(7) Loop Communications' role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.

(8) Loop Communications has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.

(9) Loop Communications is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

(10) Loop Communications' Operating Company Number is 436L.

Amanda Proffitt

Amanda Proffitt

05/27/2026