

Robocall Mitigation Plan

Business Information

Access Technologies Inc.
1055 SE Olson Dr.
Waukee, IA 50263

Contact Information

Nicole Berry
Unified Communications Manager
515-987-6227
nberry@accesssystems.com

Overview

In the Federal Communications Commission's ("FCC") 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 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

Access Technologies Inc. ("Access") is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document delineates Access's RMP. As certified in the FCC's Robocall Mitigation Database, Access has fully implemented STIR/SHAKEN. In compliance with the R&O, Access submits this RMP and certification.

Know Your Customer ("KYC")

Access's KYC program involves obtaining specific information when a subscriber signs up for service. This process includes collecting such information such as:

- name;
- phone number and outbound caller ID;
- physical business location;
- contact person(s); and
- 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, Access provides the following information concerning its upstream voice service carrier:

Bandwidth, Inc.
2230 Bandmate Way
Raleigh NC 27607
Blake Cartledge
bcartledge@bandwidth.com

Access has a master service agreement with its upstream provider. Access and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

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 Access. Access tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Access'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 Access, 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, Access will attest calls originated with these TNs.

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

Analytics for Monitoring Traffic

Access works to detect a calling pattern consistent with illegal robocalls. If such a call is 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 is involved in deploying Access's analytics.

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; and
- verifying that the call originating path is valid.

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

Access will respond to all traceback requests from the FCC, the Federal Trade Commission ("FTC"), and other law enforcement agencies as well as the Industry Traceback Group ("ITG") within twenty-four (24) hours of receiving notice of the request.

Access will investigate suspicious activity found by its monitoring systems or reported to Access by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Access 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. Access may also notify law enforcement authorities.

For all new and renegotiated Access contracts governing the transport of voice calls, Access will use best efforts to contractually require Access's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Access will implement Do Not Originate requests it receives from the ITG. If Access's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Access will take appropriate action which may include suspending or terminating the subscriber's use of Access's network. Access will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement, the FCC, and/or the ITG; as well as documenting requests & actions taken in response thereto. Too many calls that are less than 5 seconds long will cause a block from that TN. There are also numerous password policies in place to protect provisioning to our devices.

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Access 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, Access 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 Nicole Berry

I, Nicole Berry, Unified Communications Manager of Access Technologies, Inc. ("Access"), do hereby certify, under penalty of perjury, the following:

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

Access Technologies Inc.
1055 SE Olson Dr.
Waukegan, IA 50263
- (c) Access's sole dba is Access Systems.
- (d) Access has no previous dba.
- (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 following persons/entities own more than 10% of Access: Shane Sloan.
- (g) Access has no subsidiaries or affiliates.
- (h) None of the persons/entities listed herein have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (i) Access's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (j) Access has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (k) Access is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (l) Access's Operating Company Number is 010M.

/s/ Nicole Berry