

Robocall Mitigation Plan

Business Information:

Midwest Telecom of America, Inc.
1567 E. 93rd Ave.
Merrillville, IN 46410

Contact Information:

James Smutniak
Vice President
219.650.5555
jsmutniak@pickmta.com

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchoy 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 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

Midwest Telecom of America, Inc. ("Midwest Telecom") 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, Midwest Telecom has fully implemented STIR/SHAKEN. In compliance with the R&O, Midwest Telecom 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 Midwest Telecom in which we transmit, originate, and/or terminate calls on behalf of the subscriber.

New Subscribers

Midwest Telecom employees personally ensure the identity and authenticity of every new subscriber before any new subscriber is onboarded and provisioned. New subscribers go through identity verification protocols which direct communication by telephone and email with new subscribers. A Midwest Telecom employee verifies subscriber contact information, address, credit card and banking information as appropriate. A Midwest Telecom employee further ensures the identity and authenticity of each new subscriber via direct installation of services at the subscriber's place of business.

All new subscriber activity is monitored as further explained below.

Existing Subscribers

Midwest Telecom require 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. Subscriber activity is monitored as described in this document.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Ancho Seventh Report and Order In CG Docket 17-59 and WC Docket 17-9 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) **11** 49-51, Midwest Telecom provides the following information concerning its upstream voice service carrier:

Sinch Voice (dba Inteliquent, a Sinch company)
One North Wacker, Suite 2500
Chicago, IL, 60606
Gary Tabachnik
gary.tabachnik@sinch.com

Midwest Telecom's agreement with its upstream provider contains no provision specific to robocall mitigation. Midwest Telecom has, however, received assurances from its provider that it has, and will continue to, sign calls transmitted to Midwest Telecom, and will work closely with Midwest Telecom to mitigate illegal robocall traffic.

Acceptable Use Policy

Midwest Telecom maintains an Acceptable Use Policy ("AUP") that subscribers consent to as part of commercial service agreement and contractual obligation for use of the service. Subscribers must sign the commercial service agreement before being permitted to use Midwest Telecom's network. This AUP prohibits:

- 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 Midwest Telecom's service to engage in or in connection with fraudulent activities.

Midwest Telecom's contractual terms with subscribers specify that Midwest Telecom 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 Midwest Telecom and/or obtained by Midwest Telecom from one of Midwest Telecom's underlying carriers for use by the subscriber. Midwest Telecom directly manages the TNs used by its subscribers. Midwest Telecom tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Midwest Telecom's assignment of the **TN** to its subscriber.

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

Monitor Traffic with Analytics

Traffic Analysis identifies behaviors which may indicate illegal call activity. Examples of calling patterns monitored:

- Baseline alerts use historical calling data to determine a baseline and compare to current activity to determine anomalies and variances.
- Investigate whether multiple overlapping calls occur on the same account.
- Anomalies in traffic patterns indicating unusual or unexpected activities.

No third parties are involved in deploying Midwest Telecom'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;
- 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.

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

Midwest Telecom will investigate suspicious activity found by its monitoring systems or reported to Midwest Telecom by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Midwest Telecom 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 Midwest Telecom contracts governing the transport of voice calls, Midwest Telecom will use best efforts to contractually require Midwest Telecom's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Midwest Telecom will implement Do Not Originate requests it receives from the ITG. Midwest Telecom has mechanisms to automatically block suspicious calls using internal analytics. If Midwest Telecom's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Midwest Telecom will take appropriate action which may include suspending or terminating the subscriber's use of Midwest Telecom's network. Midwest Telecom 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).

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. Midwest Telecom 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, Midwest Telecom 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 James Smutniak

I, James Smutniak, Vice President of Midwest Telecom, do hereby certify, under penalty of perjury, the following:

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

Midwest Telecom of America, Inc.
1567 E. 93rd Ave
Merrillville, IN 46410
- (2) Midwest Telecom has no other business names in use.
- (3) Midwest Telecom 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) Midwest Telecom has the following owners with more than 10% interest/directors: Cary W. Smith and James Smutniak.
- (6) None of the persons listed in item 5 above have had their license denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (7) Midwest Telecom's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (8) Midwest Telecom has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) Midwest Telecom is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (10) Midwest Telecom's Operator Code Number is 919A.

/s/ James Smutniak