

Robocall Mitigation Plan

Business Information

Neometa 360, Inc.
9371 Cypress Lake Dr
Suite 6
Fort Myers, FL 33919

Contact Information

Alexander Santana
President
239-288-0029
alex@connectswfl.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 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

Neometa 360, Inc. ("Neometa") is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. Neometa is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, Neometa was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as Neometa now file RMPs. This document delineates Neometa's RMP. Because Neometa does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated herein, Neometa works closely with its upstream provider to carry out the required mitigation functions.

Know Your Customer ("KYC")

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated that subscriber. A subscriber is an entity that has a business relationship with Neometa in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Neometa's KYC program 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);
- 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 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, Neometa provides the following information concerning its upstream voice service carrier.

Neometa has one upstream provider from which it receives voice traffic:

RingLogix LLC
7735 NW 146 St
STE 202
Miami Lakes FL 33016
Gabe Olano
gabe@ringlogix.com

Neometa has a master service agreement with RingLogix LLC and has received assurances in writing from Neometa officials it has, and will continue to, sign calls transmitted to Neometa, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Neometa. Neometa and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

Neometa maintains an AUP that subscribers must sign before being permitted to use Neometa's network. Among other things, the 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 Neometa's service to engage in or in connection with fraudulent activities.

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

Mitigation During Service

Neometa works with its upstream provider to ensure that 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:

- Calls with invalid caller ID are blocked.

- Calls with matching originating and terminating numbers are blocked.
- Calls from blacklisted media IP's are blocked.
- Network monitoring for abnormal flux or call durations set off alerts and are investigated, as well as changes in customer IP addresses can set off alerts and start blocking of IP and traffic. Any inadequate response leads to removal of the route and/or MAC addresses of offending equipment.

Analytics for Monitoring Traffic

Neometa works with its upstream provider to identify behaviors which indicate illegal call activity. Examples of calling patterns monitored:

- anomalies in cost generated by calls from a single customer;
- multiple overlapping calls on the same account is a risk of not having a single subscriber using the service;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level); and
- anomalies in call duration distribution (most calls having similar duration is not representative for residential service usage).

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Neometa works with its upstream provider to follow defined procedures on investigating such subscribers.

Because Neometa does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in Neometa's analytics.

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

Neometa works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to Neometa by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Neometa contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream provider to block their use of the platform.

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

Blocking

Neometa will implement Do Not Originate requests it receives from the ITG. Neometa's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If Neometa and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, Neometa will take appropriate action which may include suspending or terminating the subscriber's use of Neometa's service. Neometa will cooperate with Investigative Bodies (provide a

single point of contact to address traceback requests from law enforcement (including the state attorney general's office), as well as 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. Neometa will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

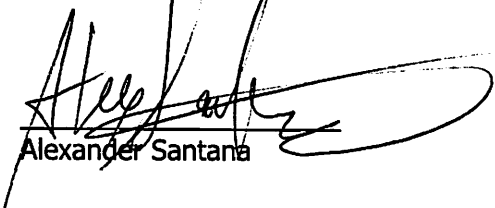
In the event of any material change to this plan, Neometa will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Alexander Santana

I, Alexander Santana, President of Neometa, do hereby certify, under penalty of perjury, the following:

- (1) Neometa, by virtue of its status as a "pure reseller" does not have access to the necessary infrastructure to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.
- (2) Neometa 's Business name and primary address are as follows:

Neometa 360, Inc.
9371 Cypress Lake Dr
Suite 6
Fort Myers, FL 33919
- (3) Neometa also operates under the business name "Connect SWFL."
- (4) Neometa has not previously used any other business name.
- (5) Alexander Santana is the only director and person owning more than 10% of Neometa. He has not had licenses/authorizations revoked by the FCC or been subject to other FCC enforcement actions.
- (6) 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.
- (7) Neometa's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (8) Neometa has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) Neometa is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.


Alexander Santana