

Robocall Mitigation Plan

Business Information

Nuacom, Inc.
1111B S Governors Ave
Ste 48555
Dover, DE, 19904 US

Contact Information

Igor Toma
CEO
+16469804718
info@nuacom.com

Overview

In the Commission's recent 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 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

Nuacom, Inc. ("Nuacom") 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, Nuacom is in the process of implementing STIR/SHAKEN with iconectiv. In compliance with the R&O, Nuacom submits this RMP and certification.

Know Your Customer ("KYC")

Nuacom maintains a strict KYC policy. We do not allow automated sign-ups; instead, all prospective customers are personally screened by our sales representatives before onboarding. Every lead must complete a mandatory phone call to verify their identity and confirm that they are located within the United States.

New Nuacom subscribers must provide name, telephone number, email address, and country. Subscribers putting money onto the Nuacom platform ("platform"), a requirement in order to place outbound PSTN calls, must also provide their credit card number and associated information. New subscribers have their outbound calls rate-limited to one per second, and human contact via phone call or in-person is required in order to increase that rate. New subscribers placing outbound calls can only use Caller IDs which have been purchased through our platform or ones ported over into our platform via our underlying carriers. Pay-by-invoice is allowed only for subscribers who we know well, with human contact via phone call or in-person at the very least, and credit and associated checks having taken place.

Human contact via phone call or in-person is required in order for new subscribers to gain access to the Nuacom platform ("platform") to make outbound calls. Subscribers deposit money into the platform via pay by card, which is a requirement before a subscriber can place outbound PSTN calls. A subscriber must provide payment through one of the following methods:

1. Online via our payment site.
2. Wire Transfer.

Nuacom is a small company, and we have a small number of customers. As a result, we know our customers and understand their use cases.

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, Nuacom provides the following information concerning its upstream voice service carrier.

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

Twilio Inc.
101 Spear Street, 1st Floor
San Francisco CA 94105
Paul Kenefick
regulatory-north-america@twilio.com

Nuacom has a master service agreement with its upstream provider and has received assurances in writing from its officials that it has, and will continue to, sign calls transmitted to Nuacom and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Nuacom. Nuacom 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")

Nuacom maintains an AUP that subscribers must agree to before being permitted to use its software and services. Among other things, the AUP prohibits:

- Using the services for any illegal, fraudulent, improper, or abusive purpose or in any way that interferes with Nuacom's ability to provide high-quality services to other customers, prevents

or restricts other customers from using the services, or damages Nuacom's or other customers' property.

- Using the Services in any manner that is illegal, obscene, threatening, harassing, defamatory, libellous, deceptive, fraudulent, malicious, infringing, tortious, or invasive of another's privacy.
- Sending unsolicited messages or advertisements, including email, voicemail, SMS, or faxes (commercial or otherwise) ("spamming"), or otherwise sending bulk and/or junk email, voice mail, SMS, or faxes without the consent of the recipient.
- Intentionally engaging in blasting or broadcasting bulk communications, advertisements, or messages (e.g., sending hundreds of messages simultaneously), including without limitation through email, voicemail, SMS, facsimile, or internet facsimile.
- Performing auto-dialing or "predictive" dialing (i.e., non-manual dialing or using a software program or other means to dial or place outbound calls continuously) in violation of applicable law or in an excessive or otherwise abusive manner.
- Creating a false Caller ID identity ("ID spoofing") or forged email/SMS address or header, or otherwise attempting to mislead others as to the identity of the sender or the origin of any communication made using the Services.
- Transmitting any material that may infringe, misappropriate, or otherwise violate the Intellectual Property rights, rights of privacy, personality, publicity, or other rights of third parties.
- Transmitting any communication that would violate any applicable law.
- Using or employing methods and/or devices designed or likely to take advantage of, bypass, exploit, or otherwise avoid compliance with the Agreement.

Telephone Number Authorization

New subscribers placing outbound calls can only use Caller IDs which have been purchased through our platform or ones ported over into our platform via our underlying carriers.

Analytics for Monitoring Traffic

Nuacom 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.

Nuacom cooperates with its upstream provider to conduct traffic analytics. No third-party vendors are involved in deploying Nuacom's analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Nuacom's 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 or her particular use case and validate that the activity belongs to that subscriber.

Nuacom follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Nuacom will devote sufficient resources to provide prompt and complete resources to traceback requests. Nuacom commits to respond within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Blocking

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

Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Nuacom will monitor industry 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, Nuacom 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 Igor Toma

I, Igor Toma, CEO of Nuacom, Inc. ("Nuacom"), do hereby certify, under penalty of perjury, the following:

(1) Nuacom is in the process of implementing STIR/SHAKEN in the IP portions of its network.

(1) Nuacom's Business name and primary address are as follows:

Nuacom, Inc.
1111B S Governors Ave
Ste 48555
Dover, DE, 19904 US

(2) Nuacom has no other business names in use.

(3) Nuacom 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) TSFY Limited (Ireland) is the 100% owner of the company. Igor Toma is the 82% owner and Mihail Mazilu is the 18% owner of TSFY Limited.

(6) The following persons exercise management and control over Nuacom: Igor Toma, Ion Toma.

(7) Nuacom has no subsidiaries or affiliates.

(8) None of the persons/entities in items 5 – 6 above have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.

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

(10) Nuacom has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.

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

/s/ Igor Toma

Igor Toma