

Robocall Mitigation Plan

Business Information

RigNet Satcom, Inc.
6155 El Camino Real
Carlsbad, CA 92009

Contact Information

Eric Baulesh
Associate General Counsel
(720) 493-6110
Eric.Baulesh@viasat.com

Overview

This document describes the steps that RigNet Satcom, Inc. ("RigNet") is taking to meet the revised Robocall Mitigation Database filing requirements and related rules adopted in the Federal Communications Commission's ("FCC") Sixth Caller ID Authentication Report and Order, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (rel. Mar. 17, 2023) ("R&O"). The R&O requires, among other things, that a robocall mitigation plan ("RMP") must outline "reasonable steps" taken to mitigate 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 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

RigNet is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. Because RigNet lacks control of the infrastructure necessary to implement STIR/SHAKEN, it is not required to be STIR/SHAKEN compliant. This document delineates RigNet's RMP.

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 RigNet in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

New Subscribers

All new subscribers go through identity verification protocols which are a mixture of algorithmic check and manual call back. A risk score is developed to ensure the authenticity of a new subscriber. This score checks the identity marker collected during an account registration process. These include but are not limited to: name, email address, credit card information and contact phone number.

These identity markers are validated for accuracy against public and paid tools. All new subscriber activity is monitored as further explained below.

Existing Subscribers

RigNet 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.

Know-Your-Upstream Providers

NovoLink Communications, Inc.
699 South Friendswood Drive
Ste 103
Friendswood, Texas 77546
281-652-4800 Main #
281-652-4802 Fax
Attn.: Jeremy Thames
NOC Manager
2816524888
regulatory@novolink.com

Lumen Technologies, Inc.
100 Century Link Drive
Monroe, LA 71203
DL-Fraud@lumen.com
866-434-2555
Attn.: Philip Linse
Director Public Policy
660 N Capitol Street NW Suite 240
Washington DC 20001
3037073844
philip.linse@lumen.com

RigNet has no contractual provisions with its upstream carriers regarding robocall mitigation, but RigNet and its upstream provider work together to mitigate illegal robocalls, including cooperating fully when receiving traceback requests. NovoLink Communications, Inc. is fully STIR/SHAKEN compliant, and Lumen has partially implemented STIR/SHAKEN, as shown in the FCC's Robocall Mitigation Database.

Acceptable Use Policy

RigNet maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use RigNet's network. Among other things, 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 RigNet's service to engage in or in connection with fraudulent activities.

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

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

Mitigation Through Contracts

All subscribers agree to participate in traceback requests (this is part of the Terms and Conditions which users must agree to when creating an account with us).

During Service

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) by requiring authentication to initiate any call, or a whitelist of originating numbers that is under the subscriber's control.

Monitor Traffic with Analytics

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

RigNet works with its upstream providers to investigate suspicious activity found by their monitoring systems or reported to RigNet by subscribers or third parties.

Dynamic Traffic Analysis identifies 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, 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.

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

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

Blocking

Where administratively feasible, RigNet will implement Do Not Originate requests it receives from the ITG. RigNet has mechanisms to automatically block suspicious calls using internal analytics. If RigNet's monitoring systems identify 4 suspected robocalling patterns that are confirmed with further investigation, RigNet will take appropriate action which may include suspending or terminating the subscriber's use of RigNet's network. RigNet 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), to 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. RigNet 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, RigNet 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 Robert Blair

I, Robert Blair, President and Secretary of RigNet, Inc. ("RigNet") do hereby certify, under penalty of perjury, the following:

- a. RigNet is not required to implement STIR/SHAKEN, due to its lack of control over the necessary infrastructure.
- b. RigNet's business name and primary address are as follows:

RigNet Satcom, Inc.
6155 El Camino Real
Carlsbad, CA 92009

- c. RigNet has no other business names in use in connection with the voice services referenced.
- d. RigNet has not previously used any other business name in connection with the voice services referenced.
- 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. RigNet's ownership is as follows:
 - i. Parent Company: Viasat, Inc.
 - ii. Entities with 10% or more ownership in RigNet, Inc.: Viasat, Inc.
- g. A list of Viasat, Inc.'s subsidiaries are included within Viasat's 10K, here: <https://investors.viasat.com/financial-information/sec-filings>
- h. RigNet's role in the call chain is that of a voice service provider with no STIR/SHAKEN implementation obligations.
- i. RigNet is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- j. RigNet has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- k. RigNet is not required to, and does not have, an Operator Code Number.

/s/ Robert Blair _____
Robert Blair