

RFCNET, INC.

Robocall Mitigation Plan

9.10.25 v1

Introduction

This document details the reasonable steps and actions taken by RFCNET, INC. ("RFCnet") to mitigate and eliminate illegal robocalling. RFCnet has an ongoing commitment to scan for and help alleviate illegal robocalling by pre-qualifying prospective customers, monitoring existing customers for traffic patterns indicative of prohibited robocalls, and working with other providers and regulatory agencies in combating fraudulent voice activity.

RFCnet is a small service provider that works with end user business customers to provide on-premise cloud-based PBX solutions. RFCnet operates their own soft switch and connects with a total of (4) service providers. Our providers are Sinch, Bandwidth, Telnyx & Commio.

STIR/SHAKEN Compliance

RFCnet is fully STIR/SHAKEN compliant and has registered with the STI-PA using OCN 306L. We have our own STIR/SHAKEN certificate and use that certificate when authenticating calls we originate.

Know Your Underlying Provider

RFCnet has master service agreements with Sinch, Bandwidth, Telnyx & Commio. All providers are fully STIR/SHAKEN compliant and will abide by the FCC's STIR/SHAKEN and robocall mitigation rules in all respects when providing services to RFCnet.

Know Your Customer

RFCnet has a 'know your customer policy' to prevent our services from being used to originate illegal traffic. We extensively investigate potential business customers seeking to access origination services prior to providing service by collecting information such as their physical business location, contact person(s), state or country of incorporation, federal tax ID, and the general nature of their business.

In our research of the prospect, RFCnet will not activate clients that provide anonymous information or where data mismatches are found. Additionally, prospects are required to agree to RFCnet's strict policies and contractual terms prohibiting the act of fraudulent voice activity as a condition of doing business with RFCnet.

Individuals associated with prospects or current customers who have been known to act improperly or otherwise be involved in fraudulent robocalling will cause their companies to be rejected by RFCnet as a customer and any existing customer relationships could potentially be severed.

Traceback Requests

RFCnet is committed and will respond fully within 24 hours to all Traceback Requests from the FCC, law enforcement agencies, and the industry traceback consortium and vows to cooperate with these agencies in investigating and stopping any illegal robocallers that use our service to make calls. RFCnet will devote sufficient resources to provide prompt and complete information to traceback requests. Our point of contact to handle all traceback requests is:

Robert Frantik
President
rfrantik@rfcinc.com

Upon contacting our dedicated Traceback Contact, we will open a case to investigate the request and extract the necessary related logs.

If a traceback exposes an existing customer as the source of fraudulent robocalls, or as having transmitted fraudulent robocalls, a demand for an explanation and verification of mitigation of the traffic is issued to the customer. If the fraudulent traffic is not remediated, RFCnet immediately begins rejecting all traffic from the offending customer.

Telephone Numbers

All new clients to RFCnet must submit an invoice or bill from their current provider that includes the telephone numbers that they want to port to RFCnet's service. From there we create an LOA form that all clients are required to sign. Numbers are verified in the carrier database to confirm they match the documentation provided. All customer requests for new numbers or porting of numbers are handled manually by RFCnet support staff. All submitted numbers will be manually called to confirm routing and answer points. All numbers will be verified to comply with DNO requirements.

International Calling

RFCnet is not currently an international voice services provider. If at any time RFCnet does decide to sell our services to international customers using North American Numbering Plan resources, we will familiarize ourselves with and develop best practices for full vetting of such customers and work with our underlying provider to perform the necessary telephone number validation on all international originated calls.

Call Analytics

RFCnet monitors switched traffic volume and logs daily for abnormal patterns. This is both to confirm expected nominal performance of our systems and to watch for abnormal/fraudulent traffic. RFCnet maintains soft switch CDR records and utilizes a 3rd party QOS monitoring system that also maintains its own call logs. These resources provide enough information for RFCnet to trace any called placed across its network back to the source.

All upstream providers monitor traffic with automated systems and will notify RFCnet of all high volume or illegal activity.

All calls subject to analytics-based call filtering will be sent the appropriate 603+ notification.

Ongoing Robocall Mitigation

RFCnet monitors and examines call detail records (CDRs) on a repeating basis to detect suspicious call activity and/or calling patterns. When we and/or our underlying provider detect network usage patterns consistent with illegal robocalls or suspect illegal robocalling is taking place, we will immediately seek to identify the party that is originating, terminating, or routing these calls so that we may take appropriate action. The actions taken may include, but are not limited to initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate and/or d/b/a name; block the party's ability to originate, terminate, or route calls on the network; and/or providing notice to law enforcement authorities.

While our soft switch platform is fully featured and fully capable of providing our customers with any service, feature or function they may need... RFCnet differs in our approach to system administration for clients. RFCnet clients do not administer their

own systems at the call routing level. RFCnet presents systems to its clients as turnkey solutions with our white-glove style of administration included. Any client that needs a change made just needs to alert our support staff. Client requests generate support ticket requests that are then reviewed and executed by members of our support team. Clients do NOT have the ability to change their routing, Caller-ID settings, etc.

RFCnet requires all business customers to sign contracts that contain provisions that allow for termination in the event origination services are abused by new and renewing customers. RFCnet will not hesitate to enforce them if necessary.

Regulatory History

RFCnet has no prior investigations, enforcement actions, or violations related to robocalls, spoofing, or related FCC regulations.

Robocall Mitigation Database (RMD) Compliance

- RFCnet has filed a certification in the FCC's RMD.
- All filings will be updated within 10 business days of any changes.

Ongoing Compliance & Review

- RFCnet's Robocall Mitigation Plan will be reviewed annually or as regulatory changes occur.
- Policies will be updated to reflect FCC guidance, industry best practices, and evolving trends.

RFCnet Contact for Robocall Mitigation-Related Issues

Please direct any questions related to Robocall Mitigation issues to:

Robert Frantik, President
RFCnet, Inc.
2368 Corporate Lane Ste 114B
Naperville, IL 60563
630-544-3150
rfrantik@rfcinc.com