

Red Spectrum **Communications, LLC**
Robocall Mitigation Plan



RED·SPECTRUM
C O M M U N I C A T I O N S

Introduction

This document details the reasonable steps and actions taken by **Red Spectrum Communications, LLC** (“Red Spectrum” or “Company”) to mitigate and eliminate illegal robocalling. Red Spectrum 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 combatting fraudulent voice activity.

Red Spectrum provides retail point-to-point data services and Voice over Internet Protocol (“VoIP”) calling services. All telecom services are provided on a resale-only basis. The Company, therefore, is exempt from the requirement to implement STIR/SHAKEN because, as a reseller, it lacks control over the network infrastructure necessary to implement STIR/SHAKEN. See *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3241, para. 40; 47 CFR Section 64.6304(b). As further detailed herein, the Company has taken steps appropriate for, and required of, a reseller to mitigate robocalling. As a telecom reseller, Red Spectrum is dependent on our underlying provider’s assistance with monitoring their networks for fraudulent voice calling patterns. Our underlying VoIP provider is Native Network Inc.

Know Your Underlying Provider

Red Spectrum has a master service agreement with Native Network Inc and has received written assurances from their officials that it has and will continue to sign calls submitted to Red Spectrum and will abide by the FCC’s STIR/SHAKEN and robocall mitigation rules in all respects when providing voice services to Red Spectrum. Red Spectrum and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Know Your Customer

Screening interviews are performed to understand potential customer business models and the potential, or lack thereof, for involvement in fraudulent robocalling schemes. Red Spectrum then performs a physical location validation check with a face-to-face visit. We also perform a credit check which includes DUNS prior to providing any service.

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

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 Red Spectrum as a customer and any existing customer relationships could potentially be severed.

Traceback Requests

Red Spectrum 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. Red Spectrum will devote sufficient resources to provide prompt and complete information to traceback requests. Our point of contact to handle all traceback requests is:

Justin Hall
Network Administrator
208-686-2080

Upon notifying our dedicated Tech Support Department, an initial ticket is opened with Network Operations. This request is then routed to the switch operator and Management is notified. We will then identify if calls apply to originating DID rules and extract the logs in question.

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, Red Spectrum immediately begins rejecting all traffic from the offending customer.

Telephone Numbers

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 Red Spectrum and/or obtained by Red Spectrum from Red Spectrum’s underlying carrier for use by the subscriber. Numbers can also be allocated by Red Spectrum or ported using information from previous bill matching customer information.

For subscribers with multi-line telephone systems, Red Spectrum and our underlying provider only allow calls to be connected if the originating number matches one of the TN’s assigned to the subscriber. This screening capability enables an automated and secure method of validating originating telephone numbers.

International Calling

Red Spectrum is not currently an international voice services provider. If at any time Red Spectrum 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

As a reseller, Red Spectrum must rely on our underlying provider and/or their third-party vendors to determine if originating calls should be blocked based on call analytics practices. In our efforts, Red Spectrum does monitor for calls to be sourced only from known locations and known DID's/TN's.

Ongoing Robocall Mitigation

Red Spectrum 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.

As part of our Plan to mitigate and prevent any originating robocalls, we are committed to early identification and investigation of possible robocalling conditions. Among other things, we watch for higher-than-normal subscriber traffic volume, including large bursts of traffic in small timeframes or spikes in usage. We also monitor for originating calls of short duration and low call completion percentages, originating calls with sequential called to number dialing patterns.

Red Spectrum Contact for Robocall Mitigation-Related Issues

Please direct any questions related to Robocall Mitigation issues to:

Justin Hall
111 North 8th Street
Plummer, ID 83851
208-686-2080
jhall@cdatribe-nsn.gov