

Robocall Mitigation Policy

Robocall Mitigation Compliance with TRACED Act

Date	On behalf of	Change Summary
June 4, 2021	Cedar Wireless, Inc.	Initial Version
February 6, 2024	Cedar Wireless, Inc.	Revision 2.1

Objective:	Establish and follow a policy that is compliant with TRACED Act
-------------------	---

I. Overview

This Robocall Mitigation Plan is submitted by Cedar Wireless, Inc. pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC) which require all “voice service providers” to establish a “robocall mitigation plan”. This document sets forth the Provider’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. The Provider views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network and in addition to following these steps the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

II. General Prohibition Against Illegal Robocalling

Cedar Wireless' end user services are subject to restrictions contained in its published legal notices and all executed services orders include the requirement that service is provided pursuant to its terms of service (“TOS”) requirements.

Its existing TOS prohibit activities normally associated with Robocalling including, but not limited to:

- 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; using the Cedar Wireless service to engage in or in connection with fraudulent activities

In addition, the company has updated its TOS to expressly reference the prohibition on robocalling and all current subscribers will receive notice of the publication of its updated TOS.

Cedar Wireless' end users are notified that Cedar Wireless may take action up to suspension or termination of service for violation of the TOS.

Robocall Mitigation Policy

III. Know Your Customer

Cedar Wireless utilizes the mitigation technique of “Know Your Customer.” Cedar Wireless is a small long established provider that maintains a close relationship with its subscribers. Its customers are generally small and mid-size businesses and few of its total customer base have enough call paths to generate the high volume of traffic associated with robocalling allowing us to use targeted in-house analytics to monitor, alert and apprehend suspected robocalling activities.

Cedar Wireless has set a call path level based on its average customer size. The level – referred to as “large volume calling capability” – is subject to change.

Cedar Wireless has a screening for new customers requesting service at or above large volume calling capability levels:

- We will not deploy large volume calling capability as a residential service or at an address shown in the company records as being residential
- Businesses requesting large volume calling capability must provide a tax ID and verification as to the nature of the business
- We verify addresses to look for overlapping / multiple deployed voice path subscriptions
- A Cedar Wireless representative may visit the premise of the business to verify the number of users at the location is appropriate for the volume of calling

Cedar Wireless serves a small number of long-time business end users with large volume calling capability that are being directly contacted to review with them Cedar Wireless' policies and efforts to prevent the Cedar Wireless network from being used for illegal robocalling.

IV. Traceback and Enforcement Cooperation

As noted above, the Provider will cooperate with the FCC, law enforcement and the (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, the Provider will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback request received within 24 hours after receiving the same. Within **Appendix A** to this Plan, the Provider identifies a single point of contact for receiving all traceback requests.

As part of its efforts to assist in the successful traceback of illegal robocalls, the Provider will going forward include within its carrier interconnection and/or service agreements language requiring traceback cooperation on any voice service calls exchanged. In part, these related contract provisions will specify the need for parties to promptly identify the upstream provider from which a suspected illegal robocall entered its network or the customer of the service from which the call originated.

Robocall Mitigation Policy

V. Telephone Number Validation Practices

Telephone Number Validation refers to the confirmation of the customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accord with industry best practices, the Provider has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of the Provider's services is permitted to use a telephone number as their caller identity if a number is directly managed by the Provider and/or obtained by the Provider via an underlying partner. Further, for: (1) single line voice service subscribers, both services connected via TDM or IP, the switching equipment has been set up to only accept calls from the number assigned to that subscriber; and (2) subscribers with multi-line telephone systems, for both services connected via TDM or IP, the Provider screens all originating calls and only allows calls to be connected if the originating number matches one of the numbers assigned to the subscriber. These screening capabilities enable an automated and secure method of validating originating telephone numbers.

VI. Ongoing Robocall Mitigation Practices

The Provider monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected or the Provider otherwise suspects illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it 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 name, trademark, or d/b/a name; terminating the party's ability to originate, terminate, or route calls on the Provider's network; and providing notice to law enforcement authorities.

As part of its Plan to mitigate and prevent any originating robocalls on its network, the Provider is committed to early identification and investigation of possible robocalling situations. In monitoring usage of its network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage); (2) originating calls of short duration and low call completion percentages; (3) originating calls with sequential called to number dialing patterns; (4) repeated calls made to do-not-call registry or invalid numbers; and (5) calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

VII. Third-Party Analytics

The Provider also uses third-party call analytics to further assist and prevent the origination of illegal robocalls on its network. Included in **Appendix A** is the name of the vendor(s) used along with a description of the call analytics system(s) used to identify and block illegal robocall traffic.

Robocall Mitigation Policy

Appendix A

Traceback Request Single Point of Contact:

Name: Jim Rodgers

Title: VP

Phone Number: 909-581-4640

Email Address: jrodgers@cedarwireless.com

Upstream Provider Information:

Name of Upstream Provider: Bandwidth, Sinch, and others

Nature of Business: Tandem Switch Provider; Wholesale Long-Distance Provider

Call Analytics Vendor Name and Description of System:

Name of Vendor: TransNexus

Description of the call analytics system

Cedar Wireless, Inc. utilizes a third-party “Analytics” platform provided by TransNexus to support the effectiveness of its Robocall Mitigation Plan. This includes, as examples, the use of “Telecom Fraud Prevention” and “Robocall and Telephone Denial of Service (TDos) Prevention” services, which include more specifically the use of the following methods/tools as a means of preventing and blocking fraudulent and illegal robocalls on its network: the use of CDRs and related reports for determining mitigation actions; use of SIP Analytics enabling real time traffic analysis and detection and mitigation of robocalls at origination; use of blacklisting and whitelisting to mitigate calls with specific attributes; use of CAPTCHA gateway services to distinguish whether calls are from humans or autodialers; use of a “Shield” database that screens calls at origination for calling numbers that are invalid, high-risk, or appear on “Do Not Originate” lists; and use of reputation look up services on calling numbers at origination.