

Wireless Technology Solutions, LLC

Robocall Mitigation Plan

Introduction

This document details the reasonable steps and actions taken by Wireless Technology Solutions, LLC (“WTS”) to mitigate and eliminate illegal robocalling. WTS 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.

WTS provides the most reliable and comprehensive primary, backup, and emergency communications for remote and multi-site environments using 4G/5G wireless data, VoIP, and advanced messaging. Our voice service is provided as an emergency/disaster recovery service only. WTS works with our provider partners with monitoring our network for fraudulent voice calling patterns.

Know Your Upstream / Downstream Providers

Wireless Technology Solutions, LLC has a master service agreement with Sinch Telecommunications (FKA Inteliquent) and has received written assurances from their officials that it has and will continue to sign calls submitted to Wireless Technology Solutions, LLC and will abide by the FCC’s STIR/SHAKEN and robocall mitigation rules in all respects when providing voice services to WTS. Furthermore, the Sinch engineering team trained us in their STIR/SHAKEN deployment and provided a detailed overview about how they support our traffic now, and the necessary process for them to manage our certificate soon. WTS and Sinch have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Know Your Customer

Besides financial vetting, we only provide voice service as an emergency/disaster recovery service. Customers must fall into our service offering criteria for us to agree to provide our products to them.

We further confirm the physical address prior to delivery to guarantee 911 service applies. We control and own the end user devices that connect to our switch. All configuration and admin access is controlled by our company and never shared with the end user. IP location and source are placed on a whitelist so the device cannot be moved without our approval.

- 1- We control and own the end user devices. No configuration credentials are shared with the end user.
- 2- Outbound caller ID MUST match the telephone number assigned to the user. All other calls will be dropped and denied access to outbound phone service.

- 3- Our downstream provider and supplier of the telephone numbers does the same filtering on outbound calls.
- 4- Traffic from the end user will only be accepted from registered endpoints and from IP addresses that are on our network whitelist.

Traceback Requests

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

Don Latimer

CTO

dlatimer@wtsolutionsllc.com

Kevin Poole

Director of IT

kpooles@wtsolutionsllc.com

Nick Rodriguez

Provisioning Manager

nrodriguez@wtsolutionsllc.com

Our team takes to call details (to from TN and Time of Day of call). With that we pull the CDR(s) pertaining to the call and share the information with the requesting party.

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, WTS 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 WTS and/or obtained by WTS from WTS's underlying carrier for use by the subscriber. Numbers

can also be allocated by WTS or ported using information from previous bill matching customer information.

For subscribers with multi-line telephone systems, WTS 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

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

WTS does not use any third parties to analyze our traffic. Our internal process is that outbound calls from our customers are limited to three standing calls. Additional calls are blocked. Our system detects short duration calls and alerts our network operations team for further investigation. International calling is blocked by default. Our system also has CDR reporting in the dashboard.

Ongoing Robocall Mitigation

WTS 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 provider partners 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. Our phone switch does not accept random SIP traffic. Our network only accepts traffic from trunks from our downstream provider and registered SIP endpoints that we own, configure and control. Traffic is limited to three standing calls per endpoint.

WTS Contact for Robocall Mitigation-Related Issues

The Company will update our Robocall Mitigation filings within 10 business days of any change to the information outlined in this plan. Please direct any questions related to Robocall Mitigation issues to:

Donald Latimer, CTO and EVP of Engineering
2100 Quaker Pointe Dr. Suite 205
Quakertown, PA 18951
610-810-3699
dlatimer@wtsolutionsllc.com