

Robocall Mitigation Program of Whidbey Telephone Company

Whidbey Telephone Company (the “Company”) is a “small voice service provider,” as that term is defined in Section 64.6304(a)(2) of the rules of the Federal Communications Commission (the “Commission”).

The Company may also be considered to be an intermediate provider, as that term is defined in Section 64.6300(g) of the Commission’s rules, with respect to traffic transiting its network and originated by, or terminated to, end users of Hat Island Telephone Company, a “small voice service provider” (as that term is defined in Section 64.6304(a)(2) of the Commission’s rules) that is under common management with the Company.

Company Network

The Company’s network consists of (i) one or more portions that originate calls in Session Initiation Protocol (“SIP”) (hereinafter “IP-capable”) and (ii) one or more portions that rely on technology that cannot initiate, maintain, carry, process and terminate SIP calls (“non-IPcapable”). With respect to the portion(s) of the Company’s network that are non-IP-capable, the Company has a continuing extension pursuant to Section 64.6304(d) of the Commission’s rules.

With respect to those portion(s) of the Company’s network that are IP-capable, the Company has, to its understanding, implemented the STIR/SHAKEN authentication framework in accordance with the Commission’s rules and orders applicable thereto¹ by subscribing to and using Metaswitch’s Call Guardian Authentication Hub, which is described as combining Metaswitch’s QCall for STIR / SHAKEN and Call Guardian Real-time Analytics of Transaction Network Services (“TNS”).

In addition, with respect to both the IP-capable portions of the Company’s network and the nonIPcapable portions of the Company’s network, the Company has implemented a robocall mitigation program that includes the following elements:

Reasonable Steps To Avoid Originating Illegal Robocall Traffic

- (a) The Company follows best practices for vetting the identity of subscribers to voice services that it provides, identified more fully under Best Practice #1 set forth in Appendix A to Public Notice DA 20-1526, released December 22, 2020, by the Wireline Competition Bureau of the FCC in WC Docket Nos. 17-97 and 20-324 (“DA 20-1526 Appendix A”).
- (b) As an originating voice service provider, all telephone numbers that are capable of originating calls on the Company’s network are assigned by the Company and,

¹ The Company understands the term “STIR/SHAKEN authentication framework,” as used in Section 64.6300 of the Commission’s rules as of the date of this document, to refer to a specific authentication framework, namely, the framework described more fully in Paragraph 21 and Note 90 of the Commission’s Sixth Report and Order and Further Notice of Proposed Rulemaking (FCC 23-18) in WC Docket No. 1797.

accordingly, consistent with the first paragraph of Section 3.4 of the NANC Call Authentication Trust Anchor Working Group Report, attached as Appendix B to DA 20-

1526,² it is the Company's understanding that originating telephone number validation, as contemplated by Best Practice #2, as set forth in DA 20-1526 Appendix A, is not needed.

- (c) The Company has procured a continuing right to use, and the Company does use, a Metaswitch-provided capability inherent in the Company's switch to monitor, in real time, the origination of interswitch, voice service calls on the Company's network, so as to trigger Company investigation of suspicious call patterns (see Item (d) below), with the goal of preventing or minimizing the origination of illegal, voice service robocalls. In addition, the TNS Call Guardian Authentication Hub provides, on a query/response basis, telephone-number-based reputation scores for any of the Company's lines.³
- (d) The Company has implemented a practice of promptly investigating calls identified by or to it as suspicious, so as to determine if the caller was attempting to originate unlawful robocalls.
- (e) The Company has established as a practice that, if the Company determines that a caller was attempting to originate unlawful robocalls, the Company will either (i) warn the subscriber to the line from which the calls originated to stop originating such calls or (ii) if permitted by law, terminate the offending service, whichever is considered to be more appropriate under the circumstances.

Do-Not-Originate (DNO) list

We maintain a **reasonable Do-Not-Originate (DNO) list**, including inbound-only government and customer-designated numbers. Calls identified with DNO caller IDs are blocked in real time across all origination, transit, and termination points in accordance with the FCC's Eighth Report & Order."

² "Telephone Number (TN) Validation refers to the confirmation of the End-User's right-to-use the telephone number. TN Validation is necessary and appropriate when an End-User's right-to-use the telephone number is unknown to the OSP responsible for performing SHAKEN attestation for the call. TN Validation is the inherent result of an OSP's assignment of a telephone number to its End-User. Thus, TN Validation may not be necessary as an explicit process in this regard." DA 20-1526, Appendix B, § 3.4 at p. 13.

³ As used here, the term "reputation score" refers to the reputation score made available to the Company by the TNS Call Guardian Authentication Hub and described more fully at the following URL: https://tnsi.com/wp-content/uploads/2022/09/CM_CallGuardian_GBL_APR2022.pdf. A copy of that webpage, as it currently exists, is attached hereto.

Our network systems integrate industry-standard DNO databases utilizing TNS CGAH (Call Guardian Authentication Hub) and when invoked the calls are blocked.

By submitting this RMP, Whidbey Telephone Company certifies that it has implemented reasonable DNO blocking measures across the network and is compliant with the FCC's Do-Not-Originate requirements and Robocall Mitigation Database filing obligations.

603+ Compliance

We have verified with our switch vendor that we are compliant with the FCC requirement to return 603+ when blocking calls using analytics (FCC 25-15). Thus, making every effort to control illegal spam and fraud calls in accordance with the FCC's Eighth Report & Order."

Know Your Customer

The Company has two principal classes of customers for services subject to the Commission's robocall mitigation rules set forth in Sections 64.6301 through 64.6308 of the Commission's rules: (i) retail, end user, voice service customers for exchange services; and (ii) switched access services customers. The Company has "know your customer" programs for each of those two classes of customers. That program for retail, end user, voice service customers consists of the practices more fully described above in paragraph (a) under the heading "**Reasonable Steps To Avoid Originating Illegal Robocall Traffic.**" The "know your customer" program for access services customers includes the practices described below under the heading "Know Your Upstream Provider."

Know Your Upstream Provider

The Company has implemented a "know your upstream provider" program with respect to the Company's immediate upstream providers of services subject to the Commission's robocall

mitigation rules set forth in Sections 64.6301 through 64.6308 of the Commission's rules. These upstream providers generally fall into one or more of three categories: (i) incumbent local exchange carriers whose switches in the public switched network are either directly subtended by the Company's switch(es) or otherwise connected by direct trunks to the Company's switch(es); (ii) interexchange carriers whose switches are connected to the Company's switch(es) by direct trunks; and (iii) non-incumbent local exchange carriers and wireless carriers that exchange local traffic with the Company by way of direct trunk groups by which their switches are connected to the Company's switch(es). To the extent feasible, the following information is collected, ascertained from one or more third-party sources, verified and/or confirmed with respect each carrier in any of those categories of providers: carrier name, carrier physical business address and/or other physical location identifier, contact person(s), state or country of incorporation or other legal formation and the provider's listing and certification in the Robocall Mitigation Database.

Contract and Tariff Provisions

The Company's services to end user customers and switched access service customers are subject to applicable tariffs, while the Company's interconnection and traffic exchange with nonincumbent local exchange carriers and wireless carriers, to the extent known to the Company, is subject to carrier-specific agreement. The Company's tariffs prohibit unlawful or abusive use of

its services.⁴ The Company's interconnection and traffic exchange agreements similarly prohibit use of the Company's services for unlawful purposes and/or require compliance with all applicable federal, state and local laws, ordinances, rules and regulations applicable to the parties' performance thereunder, and its agreement(s) for interconnection and exchange of traffic entered

into since commencement of the Commission's Robocall Mitigation Database include one or more provisions specifically addressing robocall traffic, consistent with the Commission's rules at the time such agreement was entered into.

Commitments

(a) In its capacity as a provider of "voice service," as that term is defined in Section 64.6300(n) of the Commission's rules, the Company is committed to responding within 24 hours to all lawful traceback requests from the Commission, law enforcement, and the industry traceback consortium, and, to the extent permitted by law, to cooperating with such entities in investigating and stopping the origination on the Company's voice services network of illegal robocalls by any illegal robocallers that use any of the Company's services as voice service provider to originate illegal robocalls. illegal robocalls by any illegal robocallers that use any of the Company's services as a voice service provider to originate illegal robocalls.

(b) If the Company is deemed by the Commission to be an "intermediate provider," as that term is defined in Section 64.6300(g) of the Commission's rules, in that capacity the Company is

committed to responding within 24 hours to all lawful traceback requests from the Commission, law enforcement, and the industry traceback consortium, and, to the extent permitted by law, to cooperating with such entities in investigating and stopping the use of the Company's services in that capacity to carry or process illegal robocalls by any illegal robocallers.

Dated: March 16th, 2026

⁴ The Company is an issuing carrier of National Exchange Carrier Association Tariff FCC No. 5. Section 2.2.2 of that tariff prohibits use of service furnished pursuant to that tariff for an unlawful purpose or in an abusive manner, and Section 2.1.8 of that tariff provides for termination, under certain circumstances, of services furnished pursuant to that tariff in the event of such unlawful or abusive use. The Company's local exchange service tariff(s) provide for discontinuance of service in accordance with WAC 480-120-172, which includes, as cause for discontinuance of service, "[u]nlawfully using service or using service for unlawful purposes."

TNS Call Guardian

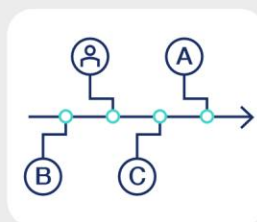
Protect Your Subscribers by Delivering Real-time Reputation Profiles

TNS Call Guardian is an industry-leading solution that uses real-time call events combined with crowd-sourced data to create accurate and comprehensive reputation profiles differentiating legitimate users of communications services from abusive, fraudulent and unlawful users.

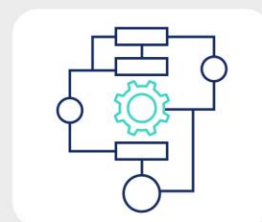
- **Accurately** detect robocalls and caller ID spoofing to help subscribers avoid answering unwanted and scam calls
- Stop **scammers** by delivering reputation profile and help subscribers avoid unwanted fraudulent calls
- Empower subscribers with a visual warning of **suspicious** callers
- Safeguard that legitimate local calls go through with **neighbor** spoofing detection
- Ensure subscriber information is **securely** protected

Report a robocall at our website,
reportarobocall.com

TNS Call Guardian is the most accurate reputation profile solution in identifying call spoofing and unwanted robocalls in real-time. The platform uses a layered approach and big data analytics to deliver reduced costs and a better customer experience for carrier subscribers.



Data Sources



Machine Learning Algorithm

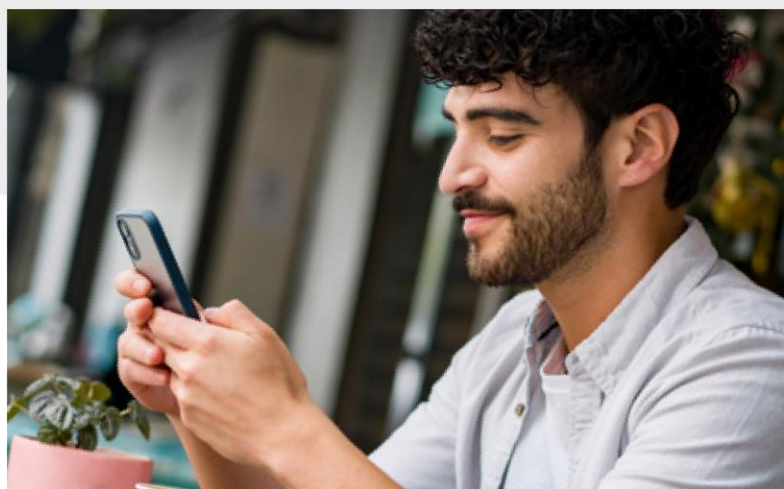


Real-time Robocall +/- Scoring



Block Fraudulent Calls

The FTC received 4.1 million robocall complaints in 2021, up from 4.1 million the prior year. Robocall bad actors continue to adjust their strategy to elude detection. The time is now to improve your subscribers' call experience.



Features

- **Insight** - Analysis of over 1 billion call events daily across more than 500 operators.
- **Reputation profiles** - Caller reputation on over 1 billion telephone numbers.
- **Real-time scoring** - Detect problems as they occur.
- **Accuracy** - High quality of identifying bad actors, including neighbor spoofing.
- **Layered approach** - Support for Do Not Originate, invalid, unallocated, unassigned numbers, STIR/SHAKEN and big data analytics using machine learning.
- **Crowd-sourced feedback** - To supplement analytics.
- **Security** - Doesn't require access to subscriber contacts.

Benefits

- **Reduce calls into customer care** - Provide your subscribers with caller reputation of incoming calls and reduce the calls into your care organization to report spam.
- **Reduce customer churn** - Decrease the chance of your subscribers falling prey to scams and fraud.
- **Increase Net Promoter Score** - Provide your subscribers with the tools to combat unwanted calls.
- **Privacy** - Protect the privacy of your subscribers, doesn't need access to subscriber contacts.
- **Reduce network costs** - Doesn't require simultaneous ring or honeypots to identify bad actors.
- **Ubiquitous solution** - Supports multiple network protocols (SIP, AIN, ENUM, Wireless) and integrates with major Telecom Application Servers.



The Most Trusted Partner for Solutions for Telecommunication Carriers or Providers

TNS addresses the evolving needs of network operators around the globe. As the industry evolves to IoT and 5G technologies, TNS leads the development of solutions to help carriers navigate a host of infrastructure complexities and maximize their network reach through the creation of unique multi-service hub solutions.

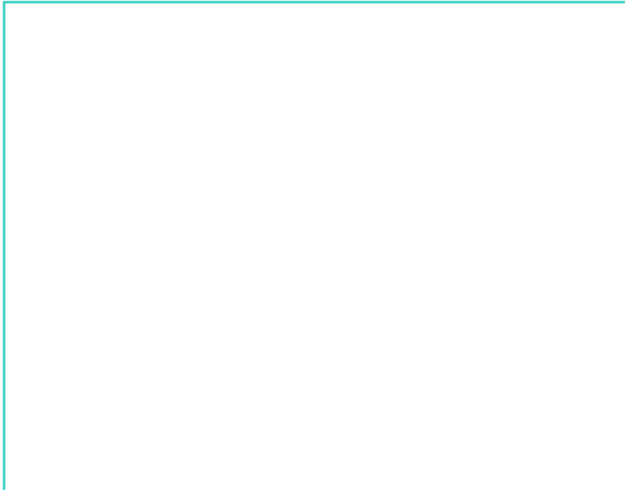
To find out more about how TNS can help you with a wide range of telecom solutions:

solutions@tnsi.com
tnsi.com

USA	+1 703 453 8300
Europe	+44 (0)114 292 0200
Asia Pacific	+61 2 9959 0800



MAR 2022
©Copyright 2022, Transaction Network Services.
All Rights Reserved.



Appendix A
Principals, Affiliates, Subsidiaries and Parent Companies

Shareholders:

2012 George TF Henny Trust

2012 Julia Henny DeMarMni Trust

2012 Mark P Henny Trust

Ian P Henny Irrevocable Trust

Julia F Henny

George TF Henny

Estate of Mark P Henny

Directors/Officers:

Steve R Winslow

Julia F Henny

George TF Henny

Donna E Hilty

Gary W Ricketts

Parent Company/Subsidiaries/Affiliates:

Abound Ventures, Inc

Western Long Distance, Inc American

Alarm Systems, Inc Fibercloud, Inc.

March 16th, 2026