

Introduction

Date: 3/25/26

Salish Networks is a voice service provider, providing Residential and Business voice services to the Tulalip Reservation. By Fully implementing STIR/SHAKEN authentication Salish Networks is reducing unwanted Robocalling if not eliminating it.

Salish Networks has a continuous commitment to recognizing and eliminating illegal robocalling through pre-qualifying future customers and monitoring traffic for prohibited robocalls. Salish Networks also works with our uplink providers to combat fraudulent voice activity. No automated sign-ups are permitted without human verification of the person's identity creating the account along with discussing with the user on how the system will be used and what will be displayed to the called party. Salish Networks does not sell service to international call originators using USA numbering plan. Salish Networks do not provision bulk VOIP phones for future use, but only provision VIOP phones for immediate use only minimizing the un-unallocated phones. Salish Networks also blocks foreign countries IP's registering their SIP phones with our Salish Networks SIP registrar.

Implementation of STIR/SHAKEN

Salish Networks has eliminated all TDM trunks and replaced them with SIP trunks making its network a true IP network. Neustar/Transunion is the STIR/SHAKEN Certificate issuer for Salish Networks. Salish Networks uses a third-party vendor-Sinch/Inteliquent carrier-to sign its calls and does not have its own token. Salish Networks hands off all outgoing/incoming traffic to Sinch/Inteliquent who subscribes to "STIR/SHAKEN and Robocall "in their IP network and this acts as another layer of protection for Salish Networks.

Salish Networks fully implemented the STIR/SHAKEN authentication framework across the entire IP portion of its network, all calls it originates are compliant with § 64.6301(a)(1) and (2).

This compliance is by virtue of Salish Networks 's underlying service providers being STIR/SHAKEN compliant within the IP portions of their networks.

Salish Networks does not allow its customers to spoof CallerID, so any outgoing CallerID can easily be traced back to the Salish Networks customer. We manage outbound CallerID ensuring all caller ID's are under the control of the entity placing the call or that in the case of call forwarding that the original caller ID may be passed, we do not allow arbitrary caller ID's to be configured or used or by users.

Compliance

Salish Networks has not been a subject of a regulatory agency action or investigation with accompanying findings of actual or suspected wrong doing due to the filing entity transmitting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

The person within the Company responsible for addressing all robocall mitigation-related issues,

Name: Tonya Payne

Title: Budget & Regulatory Analyst

Phone Number: 360-716-8013

E-mail: info@salishnetworks.com

Tracing Calls

Salish Networks is committed to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Engineer handling traceback requests:

Name: Isam Fares

Title: SR. Telecom Engineer

Phone: 425-471-2503

E-mail: SalishNOC@salishnetworks.com

Ongoing Mitigation Practices

Salish networks will investigate suspicious calls and calling patterns. If Salish networks detects a pattern consistent with illegal robocalls, or if Salish networks otherwise has reason to suspect illegal robocalling or spoofing is taking place over our network, Salish Networks will seek to identify the party that is using our network to originate, route, or terminate these calls and take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the CallerID number, determining whether the CallerID 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, route, or terminate calls on its network, and notifying law enforcement authorities.

Updating Salish Networks RMD and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5), Salish Networks will update its submission in the RMD within 10 business days of any change to the applicable information it must provide and update in the RMD.

Salish has established Blacklists to mitigate robocalls with specific attributes such as calling telephone numbers, calling other countries and blocking IP addresses that are identified as robocalls.

Salish Signed a contract with Award Consulting on Feb. 24th 2026 and implemented DNO list on our Metaswitch, the list uses ITG database list and LERG Un-allocated numbers list.

Salish Updated Metaswitch software to use SIP response code 603+ to notify callers when calls are blocked using reasonable analytics an FCC requirement (FCC-25-15).

Salish Networks RMP continues to develop as the Company and the industry gain expertise and deploy new robocall mitigation strategies and will be supplemented in future updates.