

Summit Telephone and Telegraph Company

Robocall Mitigation Plan, Version 2 Updated 2/22/2024

Certification

Summit Telephone and Telegraph Company (“Summit” or “the Company”) has not implemented STIR/SHAKEN authentication in any portion of its network. This network is non-IP and subject to a deployment extension set forth in 47 CFR § 64.6304(d) as further explained in this document.

Summit has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation within the last two years due to suspected unlawful robocalling or spoofing.

Summit has not been prohibited from filing in the Robocall Mitigation Database.

Know Your Customer

Summit Telephone and Telegraph Company (“Summit” or “the Company”) follows the best practices for vetting caller identify described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

Summit provided local service to 160 customers as of December 2020. These customers are presently served exclusively on a TDM network which limits each customer to one call path. The combination of low customer count and service over the TDM network minimizes the overall risk of Robocalls originating from the company’s customers. The Company will work with its customers that may place legitimate Robocalls to ensure their traffic is not blocked. Examples could include school districts that might Robocall to announce cancellations or delays, or electric utilities that may contact customers to report on network outages.

Know Your Upstream Provider

Summit knows all the carriers from which it receives traffic and has confirmed that all carriers in which it exchanges traffic and from which it receives traffic are listed in the Robocall Mitigation Database. Basic identification information, such as physical business location, contact person(s), state of incorporation, and nature of business, are collected for all of the Company’s up-stream providers. Going forward, all interconnection agreements will include prohibited traffic and traceback language.

Traceback

Summit responds to all traceback requests from the Commission, law enforcement and the registered traceback consortium and cooperates with such entities in investigating and stopping any illegal robocallers that use our service to originate calls. The Company's contact for traceback is:

James Perry
Acting General Manager
(907) 389-1012
jperry@summittelephonecompany.com

Robocall Mitigation Program

Summit has committed to a Robocall Mitigation Program for all originating calls made from our network using software provided by TransNexus. All outbound calls made from our subscribers will be analyzed using this software, providing real time, detailed information and reporting on all originating calls. The TransNexus software provides detailed reporting identifying suspected illegal robocalls and provides alerts if originating calls may contain a number that:

- is identified as invalid, or
- is identified as unallocated, or
- is on a Do Not Originate list, or
- is in the FCC consumer complaint database, or
- has a poor reputation score.

We will immediately investigate any potential robo or suspicious calls. If warranted, we will notify the customer to stop originating unlawful calls or face termination of their service as appropriate.

Summit has the right to terminate customers making Robocalls under the terms and conditions contained in the Company's local service tariff (APUC No. 350). The General Rule and Regulations includes a section titled Cancellation for Cause which allows disconnection of service if it is determined the service is being or will be used for unlawful purposes (*See APUC No. 350, Sheets 2.19 to 2.22*).