

NEX-TECH WIRELESS LLC

STIR/SHAKEN IMPLEMENTATION, CERTIFICATION, AND ROBOCALL MITIGATION PLAN

Pursuant to section 64.6305 of the Federal Communications Commission's ("Commission's") rules, Nex-Tech Wireless LLC ("Nex-Tech Wireless" or "Company") submits this certification and accompanying Robocall Mitigation Plan.

STIR/SHAKEN Implementation

Nex-Tech Wireless has fully implemented STIR/SHAKEN on the IP portion of its network; all such calls are compliant with section 64.6301(a)(1) and (2) of the Commission's rules.

Nex-Tech Wireless also has portions of its network that are non-IP. Currently, TDM/SS7 cannot support STIR/SHAKEN. Accordingly, the Company is subject to a continuing extension as set forth in Section 64.6304(d) of the Commission's rules, which is relevant to those "portions of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls." Nex-Tech Wireless is a member of CCA, which are actively participating in industry efforts to develop a non-IP solution to illegal robocalls. When industry standards are established and software/hardware is commercially available to support these standards, the Company will then implement these robocall mitigation standards for the non-IP portions of our network.

Identifying and Other Information

Primary address:

Nex-Tech Wireless LLC
3001 New Way
Hays, KS 67601

Affiliates: None

Principals of Nex-Tech Wireless: Rural Telephone Service Company, Inc., Nex-Tech, LLC, GBT Communications, Inc., Golden Belt Telephone Association, Inc., TC Wireless, LLC, TC Wireless, Inc., The Tri-County Telephone Association, Inc.

The Company is not a foreign voice service provider.

OCN: 122D

Individual responsible for addressing robocall mitigation-related issues:

Nathan Sutter, Vice President of Technology
Networking Department
3001 New Way
Hays, KS 67601
Phone: 785-621-3650
E-mail: nsutter@ntwls.com

Enforcement

All calls that originate on the Company's network are subject to the attached Robocall Mitigation Plan.

Nex-Tech Wireless has never been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program.

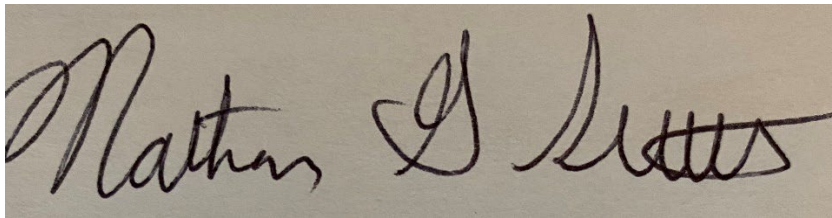
Nex-Tech Wireless has not been prohibited by the Commission from filing in the Robocall Mitigation Database.

Traceback

Nex-Tech Wireless will respond fully within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use its service to carry, process, or originate robocalls.

I, Nathan Sutter, Director of Network Operations and Engineering, submit this certification on behalf of Nex-Tech Wireless LLC, which has implemented the STIR/SHAKEN authentication framework as indicated in the Robocall Mitigation Database.

Pursuant to section 1.16 of the Commission's rules, I certify, under penalty of perjury that the information and statements contained herein are true and correct to the best of my knowledge and belief.

A handwritten signature in dark ink on a light-colored background. The signature is written in a cursive style and reads "Nathan Sutter".

Nathan Sutter

Robocall Mitigation Plan

The policies and procedures outlined herein describe the specific “reasonable steps” Nex-Tech Wireless has taken to avoid the carrying or processing of illegal robocall traffic.

Call Analytics

Nex-Tech Wireless utilizes TNS Call Guardian call analytics to mitigate robocalls. TNS provides call monitoring, blocking, and filtering analytics from the TNS Call Guardian product to stop any callers suspected of illegal robocalling or spoofing over our network. The TNS products blocks calls originating from invalid numbers and Do Not Call numbers. The TNS product analyzes high-volume network traffic to identify and monitor patterns consistent with robocalls and provides real-time reports of suspicious activity. TNS will investigate suspicious activity and contact us. If it is determined that a customer is originating prohibited, unlawful calls on our network, Nex-Tech Wireless will take appropriate action consistent with our Acceptable Use Policy, which prohibits customers from utilizing our network for deceptive purposes, engaging in fraudulent activities, and violating local, state, or federal laws. If Nex-Tech Wireless has a reasonable basis to believe that a customer is originating illegal robocalls, the Company will require the customer to remedy the problem and, if effective action is not taken, Nex-Tech Wireless can suspend and/or terminate service to the customer.

Know-Your-Customer

Nex-Tech Wireless follows the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group at <https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>).

Nex-Tech Wireless vets new and renewing customers. Nex-Tech Wireless confirms the identity of new or renewing residential and business customers by collecting identifying information including, as applicable, SSN, date of birth, contact person for the business, physical address, state and/or country of incorporation, and federal tax ID. Nex-Tech Wireless also verifies customer’s credit history and business reputation prior to providing service. New customers requesting an excessive number of call paths will be screened for legitimate usage needs. New and existing customers with an excessive number of call paths will receive robocall outreach. All residential and business customers are only able to place calls originating from their own phone number. Caller ID and call records are reviewed when service is installed to verify legitimate caller ID information.

Know-Your-Upstream Provider

Nex-Tech Wireless knows all carriers from which it receives traffic. Nex-Tech Wireless has confirmed that all connected providers are listed in the Robocall Mitigation Database. Nex-Tech Wireless shares call authentication data with connected service providers.

Traceback

Nex-Tech Wireless will respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use our network to originate robocalls.