



ROBOCALL MITIGATION PROGRAM

Business Information

Hancock Rural Telephone Corporation, d/b/a NineStar Connect
(f/k/a Hancock Telecom, Hancock Long Distance)
2243 E. Main Street
Greenfield, IN 46140
317.326.3131

Principals, Affiliates, Subsidiaries, and Parent Company Information

Michael R. Burrow is the President & CEO of Hancock Rural Telephone Corporation d/b/a NineStar Connect and Central Indiana Communications, Inc. d/b/a NineStar Communication. Hancock Rural Telephone Corporation d/b/a NineStar Connect is the Parent Company of Central Indiana Communications, Inc. d/b/a NineStar Communications. Hancock Rural Telephone Corporation d/b/a NineStar Connect has 100% ownership and management control of Central Indiana Communications, Inc. d/b/a NineStar Communications.

Contact Information

Kimberly Gerard
Legal & Compliance Manager/Assistant Secretary
317.323.2105
kgerard@ninestarconnect.com

Purpose

This Robocall Mitigation Plan is for Hancock Rural Telephone Corporation d/b/a NineStar Connect ("NSC"), with headquarters at 2243 E Main Street, Greenfield, IN 46140. NSC is dedicated to stopping illegal calls from originating on our network and monitoring the calls coming into our network. This document delineates NSC's Robo-Call Mitigation Plan, which consists of the elements as outlined below.

NSC is eligible for the continuing extension of the STIR/SHAKEN implementation deadline as a small voice service provider (§64.6304 (a)(2) that has non-IP portions within its network §64.6304(d). NSC provides local service to fewer than 100,000 voice subscriber lines. A portion of customers are served on the non-IP portions of NSC's network which relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls. Consistent with §64.6303(a)(1), NSC is ready to upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework. However, the NSC non-IP network is connected to carriers that do not support IP connectivity; therefore, NSC cannot upgrade those Non-IP portions of its network to IP connectivity.

Additionally, to meet the non-IP network criteria for the continuing STIR SHAKEN extension (§ 64.6303 (a)(2)), Ninestar is a member of NTCA. NTCA participates on the ATIS PTSC Non-IP Call Authentication Task Force working group which developed the (ATIS Solutions) non-IP call authentication solutions. NTCA is serving as NineStar's third-party representative on the ATIS PTSC Non-IP Call Authentication Task Force working group.

STIR/SHAKEN Authentication

NSC has implemented STIR/SHAKEN in partnership with TransNexus as the STI-Certificate Authority. Through this partnership, we are participating in the attestation and 'tokening' process in accordance with the FCC mandated STIR/SHAKEN framework. TransNexus authenticates SIP calls originating on our network as STIR/SHAKEN compliant. All voice traffic that originates on our network is subject to the robocall mitigation program described below.

Robocall Mitigation Plan

- We perform the following roles in the call chain:
 - A voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- Know your customer
 - NSC has procedures in place to prevent new and renewing customers from using our network to originate illegal robocalls. NSC thoroughly vets new residential and business customers by asking personally identifiable questions for additional security on each account before activating new service or making changes to existing services. Details below:
 - Residential customers are asked to provide their full name, address (physical and mailing, if different), last four digits of their social security number, date of birth, phone number, email, and establish security questions and a password.
 - Business customers are asked to provide their full name, address (physical and mailing, if different), tax identification number, phone number, email, and establish security questions and a password. To initiate an account change, a customer must provide their password or the answer to their security question prior to initiating a change. If the customer is unable to provide that information, the customer service representative will call the customer back using the number they provided at account setup.
- Traceback
 - We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls. NSC commits to responding to traceback requests within 24 (twenty-four) hours.
- Robocall Mitigation Program
 - We use call analytics software provided by TransNexus to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls.
 - The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.
 - We perform the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call.
 - We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.
- Upstream Provider Knowledge

NSC knows all of its connected carriers and has confirmed each carrier is resident in the Robocall Mitigation Database. NSC monitors incoming traffic from all connected carriers for suspicious call patterns indicative of illegal robocall activity. The connected carriers are made aware of any suspicious or illegal traffic identified and notified that, if the traffic does not cease, the calls may be blocked from entering NSC's network. No provider in NSC's network to carry or process a high volume of illegal traffic.

- STIR/SHAKEN
 - We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that we use when authenticating calls we originate. We have implemented a STIR/SHAKEN solution supplied by TransNexus.

Acceptable Use Policy

NSC maintains an Acceptable Use Policy ("AUP") that is incorporated within the Service Contract that each customer must sign before being permitted to use NSC's network. Among other things, this AUP prohibits:

- Using the NSC network for unlawful purposes
- Engaging in conduct that is fraudulent or deceptive
- Transmitting uninvited communications

NSC's AUP specifies that a violation may result in the denial, restriction, suspension, or termination of the user's service.