

PINELAND TELEPHONE COOPERATIVE ROBOCALL MITIGATION PLAN

Pineland Telephone Cooperative (Pineland), Operating Company Number 0377, is eligible for the continuing extension of the STIR SHAKEN implementation deadline on Non-IP networks as a small voice service provider (§64.6304 (a)(2) that has non-IP portions within its network §64.6304(d). To meet the non-IP network criteria for the continuing STIR SHAKEN extension (§ 64.6303 (a)(2)), Pineland 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 Pineland's third-party representative on the ATIS PTSC Non-IP Call Authentication Task Force working group.

Pineland provides local service to fewer than 100,000 voice subscriber lines. Most customers are served on the non-IP portions of Pineland's network which relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls.

Pineland's non-IP network is connected to carriers that do not support IP connectivity; therefore, Pineland cannot upgrade those Non-IP portions of its network to IP connectivity.

Consistent with § 64.6303 (a)(1), Pineland 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. Pineland has contacted all of its connected carriers and requested to convert the Non-IP connections to IP connections. The carriers stated they cannot support IP connections at this time. Therefore, Pineland cannot upgrade those Non-IP portions of its network to IP connectivity.

Pineland's network also has IP-portions which originates calls via SIP connections to other carriers. Pineland has registered with the Policy Administrator and is an authorized service provider in the STIR/SHAKEN ecosystem. Pineland has implemented STIR/SHAKEN within the IP portions of its network and signs the calls originating on the IP portions of its network with its certificate.

Robocall Mitigation Plan

All voice traffic that originates on Pineland's network is subject to the following Robocall Mitigation Plan.

Call Analytics

scoring of our network's outbound traffic. The vendor's analytics identify patterns of suspected illegal robocalls and scores the calls based on their behavior and/or their status as suspected robocalls as reported to the Federal Communications Commission (FCC), Federal Trade Commission (FTC), and as reported by other carriers. Pineland has access to the vendor's portal and receives notifications about telephone numbers originating suspected illegal robocalls on its network, including from unassigned, inactive and do not-originate TNs. Pineland also receive reports via e-mail alerts if any of its numbers experience a change in reputation such as

suspicious traffic patterns or other detected anomalies outside the normal behavior of our company's traffic. Pineland will examine the reports and investigate and identify the source of the calls as unlawful or legitimate.

Pineland investigates calls identified by Sinch/Inteliquent as suspicious calls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

In addition, if Pineland has any other reason to suspect illegal robocalling or spoofing is taking place over its network, Pineland will work internally to identify the party that is using our network to originate, route, or terminate such calls and take appropriate action.

Illegal robocalls and fraudulent spoofing is prohibited on our network. If it is determined a Pineland customer is using our network to fraudulently spoof calls or to originate illegal robocalls, Pineland will either warn the customer to stop such practices or terminate their service as allowed per Pineland policy.

Know your Customer

Pineland has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. Pineland 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.

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 a security question, and a password. Pineland also requires a photo ID for all new customers requesting voice service.

Business customers are asked to provide their full name, address (physical and mailing, if different), tax identification number, phone number, email, and establish a security question, 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.

Upstream Provider Knowledge

Pineland knows all the carriers from which it receives traffic and has confirmed that all the carriers are listed in the Robocall Mitigation Database. No provider is using Pineland's network to carry or process a high volume of illegal traffic. Pineland 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 and notified that, if the traffic does not cease, the calls may be blocked from entering Pineland's network. In addition, Pineland is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

Traceback

Pineland commits to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that we learn are using our service to originate calls. Pineland commits to responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, within twenty-four (24) hours.