

Twin Lakes Telephone Cooperative ROBOCALL MITIGATION PLAN

Twin Lakes Telephone Cooperative 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).

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

Consistent with § 64.6303 (a)(1), Twin Lakes Telephone Cooperative 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. Twin Lakes's non-IP network is connected to carriers that do not support IP connectivity. Twin Lakes Telephone Cooperative 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, Twin Lakes cannot upgrade its Non-IP network to IP.

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

Robocall Mitigation Plan

All voice traffic that originates on the Twin Lakes network is subject to the following Robocall Mitigation Plan.

Call Analytics

Twin Lakes has contracted with **TNS** to provide robocall analytics and reputation scoring of our network's outbound traffic. The vendor uses software to monitor outbound voice traffic in real time. The software's identification of suspected illegal robocalls and alerts helps prevent the origination of illegal robocalls. We have also implemented STIR/SHAKEN with our SIP providers to add a layer of authentication for IP voice traffic.

Investigation

Twin Lakes investigates calls identified by **Metaswitch** and **TNS Call Guardian** as suspicious calls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

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

Enforcement

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

All Twin Lakes customers sign a service agreement / application before new service is activated or existing service is renewed. The service arrangement/ application includes notice that Twin Lakes prohibits use of its network for the initiation of fraudulent spoofing and robocalls and if end users are found in violate of the service terms, the end user's service may be terminated.

Know your Customer

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

For residential customers, we kindly request the following information: full name, address (physical and mailing, if different), social security number, date of birth, contact number, email, secure pay PIN, and the establishment of password and security questions. Additionally, Twin Lakes may ask for a copy of a photo ID if the customer is present in the office, but the photo ID is not mandatory.

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

Twin Lakes knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. Twin Lakes has also reviewed the connected carrier's robocall mitigation plans to learn how the carriers monitor their originating traffic to mitigate illegal robocalls. Twin Lakes does not directly receive traffic from any foreign originating or intermediate provider. No provider is using Twin Lakes 's network to carry or process a high volume of illegal traffic. In addition, Twin Lakes is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

Traceback

Twin Lakes 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. Twin Lakes commits to responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, within twenty-four (24) hours.