

Taylor Telephone Cooperative ROBOCALL MITIGATION PROGRAM

Taylor Telephone Cooperative (Taylor), OCN 2151, 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).

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

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

Taylor's network also has IP-portions which originates calls via SIP connections to other carriers. Taylor has registered with the Policy Administrator and is an authorized service provider in the STIR|SHAKEN ecosystem. Taylor 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 Program

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

Call Analytics

Taylor Telephone Cooperative, Inc. blocks calls originating from numbers that are not valid North American Numbering Plan (NANP) numbers, known numbers not allocated to a provider and numbers not assigned to a Taylor Telephone Cooperative, Inc. subscriber or otherwise set aside for outbound call use. Taylor Telephone Cooperative, Inc. monitors all originating network traffic for suspicious or abnormal call volume or activity.

Calls that meet the below qualifying factors are investigated internally to determine if the calls are legitimate or unlawful:

- High-volume voice network traffic
- Large bursts of calls in a short timeframe
- Short duration calls
- Low average call duration
- Low call completion ratios
- Sequential dialing patterns
- Neighbor spoofing patterns

Investigation

Taylor investigates all suspicious calls and those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

In addition, if Taylor has any other reason to suspect illegal robocalling or spoofing is taking place over its network, Taylor 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 Taylor customer is using our network to fraudulently spoof calls or to originate illegal robocalls, Taylor will either warn the customer to stop such practices or terminate their service as allowed per Taylor policy.

Know your Customer

Taylor has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. Taylor 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), phone number, email, and establish a security question, and a password. Taylor 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

Taylor knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. Taylor monitors incoming traffic from all connected carriers for suspicious call patterns indicative of illegal robocall activity, notifies the upstream carriers of any such traffic and warns the carriers that if the traffic does not cease, the calls may be blocked from entering Taylor's network. In addition, Taylor is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

Traceback

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