

ROBOCALL MITIGATION PLAN

North Penn Telephone Company and North Penn Long Distance Corporation

North Penn Telephone Company OCN 0192 and North Penn Long Distance Corporation OCN 091H (Company) are eligible for the continuing STIR SHAKEN implementation deadline under FCC rules §64.6304(a)(2) and §64.6304(d).

Company qualifies 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).

Company provides local service to fewer than 100,000 voice subscribers on the non-IP portions of Company's network which relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls.

Consistent with § 64.6303 (a)(1), Company is ready to upgrade its non-IP network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework. Company 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.

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

Robocall Mitigation Plan:

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

Company subscribes to Ribbon's Reputation Scoring Service to provide call analytics and reputation scoring of our network's outbound traffic. Ribbon's service uses software to monitor outbound voice traffic in real time and provides detailed reporting identifying if our network originates any calls where the calling number is invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database or has a poor reputation. Company has access to the vendor's portal and receives notifications about telephone numbers originating suspected illegal robocalls on its network. The software's identification of suspected illegal robocalls and alerts helps prevent the origination of illegal robocalls.

Company also subscribes to Ribbon's RoboProtect service which uses Nomorobo's database of known, illegal robocallers to help Company stop unsolicited and spoofed phone calls.

Investigation

Company investigates originating calls identified by Ribbon's Reputation Scoring Service as suspicious calls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

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

Know your Customer

Company has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. Company 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. Company also requires a photo ID for all new customers requesting voice service.

In addition, all end users sign a service agreement when new service is activated or existing service is renewed. The service arrangement includes notice that Company prohibits use of its network for the initiation of fraudulent spoofing and robocalls. If end users are found in violation of the service terms, the end user's service may be terminated.

Upstream Provider Knowledge

Company 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 Company's network to carry or process a high volume of illegal traffic. Company 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 Company's network. In addition, Company is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

Traceback

Company 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. Company will respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium fully and in a timely manner within twenty-four (24) hours.