

Sledge Telephone Company ROBOCALL MITIGATION PROGRAM

Sledge Telephone Company (Sledge), OCN 0466 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).

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

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

Robocall Mitigation Program

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

Internal Traffic Monitoring & Analytics

Sledge monitors all originating network traffic for suspicious or abnormal call pattern, 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

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

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

Know your Customer

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

Upstream Provider Knowledge

Sledge knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. Sledge 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 Sledge's network. In addition, Sledge is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

Traceback

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