

GRIGGS COUNTY TELEPHONE COMPANY ROBOCALL MITIGATION PLAN

Griggs County Telephone Company (Griggs), Operating Company Numbers 1615 & 1622, is eligible 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).

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

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

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

Robocall Mitigation Plan

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

Call Analytics

Griggs has contracted with TransNexus to provide robocall analytics and reputation 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. Griggs has access to the vendor's portal and receives real-time eventbased notifications about telephone numbers originating suspected illegal robocalls on its network, including from unassigned, inactive and do-not-originate TNs. Griggs also receives reports via email alerts if any of its numbers experience a change in reputation such as suspicious traffic patterns or other detected anomalies outside the normal behaviour of our company's traffic.

Investigation

Griggs investigates calls identified by its internal traffic monitoring as suspicious calls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

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

Know your Customer

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

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

Griggs knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. Griggs has also reviewed the connected carrier's RMPs to learn how the carriers monitor their originating traffic to mitigate illegal robocalls. Griggs 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 the Griggs network. In addition, Griggs is now incorporating traceback and prohibited traffic language in all contractual agreements with upstream carriers.

Role In the Call Chain

Griggs is a voice service provider with a STIR/SHAKEN implementation obligation on the IP portions of its network. Griggs is also a voice service provider without a STIR/SHAKEN obligation on the Non-IP portions of its network because that portion of the network relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls.

Traceback

Griggs 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. Griggs 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.

Robocall Mitigation Database Eligibility

Griggs has not been involved in any recent, formal law enforcement or regulatory investigation into suspected unlawful robocalling.

Griggs has not been prohibited from filing in the Robocall Mitigation Database (RMD).

Customer Education

Griggs posts information on its website to educate customers on how to protect themselves from becoming a victim of unlawful robocalls and a process to report complaints related to robocall activity.