

GLENWOOD TELEPHONE COMPANY

ROBOCALL MITIGATION PLAN

Glenwood Telephone Cooperative (Glenwood), Operating Company Number 0365, 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).

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

Glenwood's non-IP network is connected to carriers that do not support IP connectivity; therefore, Glenwood cannot upgrade those Non-IP portions of its network to IP connectivity.

Consistent with § 64.6303 (a)(1), Glenwood 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. We are currently in the process of working with Toly to provide these services.

To meet the non-IP network criteria for the continuing STIR SHAKEN extension (§ 64.6303 (a)(2)), Glenwood Telephone Company is a member of NTCA. NTCA participates on the ATIS PTSC Non-IP Call Authentication Task Force working group which developed the (ATIS Solutions) non-IP call authentication solutions. NTCA is serving as Glenwood Telephone Company's third-party representative on the ATIS PTSC Non-IP Call Authentication Task Force working group.

Robocall Mitigation Plan

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

Glenwood Telephone Company 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 time-frame
- short duration calls
- low average call duration
- low call completion ratios

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

Illegal robocalls and fraudulent spoofing is prohibited on our network. If it is determined a Glenwood customer is using our network to fraudulently spoof calls or to originate illegal robocalls,

Glenwood will either warn the customer to stop such practices or terminate their service as allowed per Glenwood policy.

Know your Customer

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

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

Traceback

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