

WEST TEXAS RURAL TELEPHONE COOPERATIVE INC ROBOCALL MITIGATION PLAN

West Texas Rural Telephone Cooperative Inc (WTRTC), Operating Company Number (2166), 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).

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

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

Robocall Mitigation Plan

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

Call Analytics

WTRTC contracts with Metaswitch and Transaction Network Services (TNS) for the Call Guardian Authentication Hub service which provides an authentication and robocall prevention solution. The service consists of call analytics (TNS Call Guardian) and STIR/SHAKEN (Metaswitch QCall), delivered as a hosted service from TNS's geo-redundant data centers.

Call Guardian is built on a data analytics engine fed by multiple comprehensive data sources. First, it leverages TNS's position in the network to see billions of calls per day from hundreds of operators. Second, it includes feedback from over 100 million users of a mobile application that can be used to report good and bad calls. Third, there is the consumer facing website reportarobocall.com, which the public can use to report bad calls. Fourth, it includes information on unallocated, unassigned and DNO (do-not-originate) numbers from hundreds of service providers. This dataset has excellent coverage of the US numbering plan, with reputation scores (from +4 for very good to -4 to the worst) and categorizations (e.g. robocaller, spammer, scammer) indicating not just the severity but also the nature of the risk inherent in answering a call from that number. The information is maintained in real time, based on patterns of behavior and explicit feedback.

The subscription includes access to the TNS Portal, which includes a number of tools for robocall mitigation.

- The *negative reputation report* provides a list of all negatively scored numbers belonging to the service provider, which can be used as a "watch list" of numbers of concern. The data can be filtered and exported as required. For any number in question, it is possible

to look at the detail, including the history of reputation changes (including reasons) and the volume of calls seen by the platform. This can be accessed at any time.

- A *batch reputation report* is available, reporting on the score and category of numbers of concern, generated on demand.
- A *reputation monitoring* feature is provided, delivering alerts for changes in reputations of telephone numbers, allowing operations staff to take action as needed. The list of numbers of concern is supplied to the platform, and then whenever the data analytics changes the reputation of a number an e-mail is sent to a specified address with the information.

In addition to features targeted specifically at robocall mitigation, Call Guardian Authentication Hub includes industry-leading support for robocall analytics for blocking, diverting and labeling calls consistently with FCC regulations and “safe harbor” provisions, with capabilities as follows:

- blocking calls that are from invalid, unassigned or unallocated numbers
- blocking calls from DNO numbers
- diverting calls to an announcement or voicemail using reasonable analytics
- updating caller name information on suspicious calls to warn the user – e.g. using the text “spam?”.

Call Guardian Authentication Hub also supports STIR/SHAKEN in compliance with the ATIS standards and applicable FCC regulations for signing and verifying calls using STI certificates.

Investigation

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

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

Know your Customer

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

Upstream Provider Knowledge

WTRTC knows all the carriers from which it receives traffic and has confirmed that all its connected carriers are listed in the Robocall Mitigation Database.

WTRTC has also reviewed the connected carrier's RMPs to learn how the carriers monitor their originating traffic to mitigate illegal robocalls.

In addition, WTRTC is now incorporating traceback and prohibited traffic language in all contractual agreements with upstream carriers.

Role In the Call Chain

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

Traceback

WTRTC 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. WTRTC 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

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

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

Customer Education

WTRTC 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.