

Arkwest Communications Robocall Mitigation Plan

Arkwest Communications - Operating Company Number 1734 - 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).

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

The Arkwest non-IP network is connected to carriers that do not support IP connectivity; therefore, Arkwest Communications cannot upgrade those non-IP portions of its network to IP connectivity.

In addition, to meet the non-IP network criteria for the continuing STIR SHAKEN extension (§ 64.6303 (a)(2)), **Arkwest** 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 Arkwest's third-party representative on the ATIS PTSC Non-IP Call Authentication Task Force working group.

Arkwest has implemented partial STIR SHAKEN in its network. Arkwest is registered with the Policy Administrator and is an authorized provider in the STIR|SHAKEN ecosystem. All VoIP traffic that originates on Arkwest's IP - network is authenticated with STIR SHAKEN and signed with the Arkwest certificate.

Arkwest Communications has implemented the following Robocall Mitigation Plan to detect and prevent unlawful robocalls from originating on its network.

All voice traffic that originates on Arkwest's network is subject to this robocall mitigation program.

Call Analytics

Arkwest uses Ribbon Communications' Call Trust solution to monitor outbound voice traffic in real time to prevent the origination of illegal robocalls. Arkwest uses Ribbon Communications' Identity Hub Service for Advanced Fraud Reputation Scoring and Advanced Nuisance Reputation Scoring. The software provides real-time scoring, detailed reporting and identifies suspected illegal nuisance or fraudulent calls. The solution allows

ArkWest to block originating 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.

Investigation

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

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

Know Your Customer

Arkwest has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. (Company Name) 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 (Company Name) 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 . 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.

Also new customers are notified of service agreement terms regarding prohibited use of Arkwest telephone numbers for illegal robocall traffic.

Upstream Provider Knowledge

Arkwest knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. Arkwest 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 identified and notified to cease the traffic or the calls may be blocked from entering Arkwest's network. No provider is using Arkwest's network to carry or process a high volume of illegal traffic. In addition, Arkwest is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

Traceback

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