



DBA Central Broadband

Central Scott Telephone Company, Inc. (FRN 0003722121), CST Communications, Inc. (FRN 0002577297), CS Technologies, Inc. (FRN 0005099619), and Dixon Acquisition LLC (FRN 0025493925)

**Policy and Procedure for Robocall Mitigation Plan
As of February 26, 2025**

BACKGROUND: The FCC requires implementation of STIR/SHAKEN, a caller ID authentication framework, to combat illegal robocalls. STIR/SHAKEN is a set of industry-created technological standards that help to prevent illegally “spoofed” calls.

The following is the definition per the FCC website: “STIR/SHAKEN is a framework of interconnected standards. STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited (“STIR”) and Signature-based Handling of Asserted Information Using toKENs (“SHAKEN”) standards. This means that calls traveling through interconnected phone networks would have their caller ID “signed” as legitimate by originating carriers and validated by other carriers before reaching consumers. STIR/SHAKEN digitally validates the handoff of phone calls passing through the complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is in fact from the number displayed on Caller ID.”¹

The FCC required voice service providers to implement the STIR/SHAKEN call authentication technology in the Internet protocol (IP) portions of their phone networks by June 30, 2021 (delayed to 2023 for small providers including our Company) per the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”).

In September 2020, The FCC completed implementation of the TRACED Act with respect to STIR/SHAKEN and required intermediate providers to facilitate caller ID authentication. The FCC adopted more rules to ensure that voice service providers unable to implement STIR/SHAKEN immediately take steps to protect their customers from illegal robocalls.

As of April 20, 2021, the FCC requires all voice service providers certify in the FCC Robocall Mitigation Database one of 3 options: 1) fully implemented STIR/SHAKEN; 2) partially implemented STIR/SHAKEN and have instituted a robocall mitigation program to ensure that they

¹ <https://www.fcc.gov/call-authentication>

are not originating illegal robocalls; or 3) not implemented STIR/SHAKEN but have instituted a robocall mitigation program to ensure that they are not originating illegal robocalls.

All providers are required to submit to this public database the contact information for the personnel at their company responsible for robocall-mitigation related issues. Providers certifying to their implementation of a robocall mitigation program are required to include descriptions of the reasonable steps they are taking to avoid originating illegal robocall traffic.

Filings in the Robocall Mitigation Database are due June 30, 2021. Finally, because the STIR/SHAKEN framework is only operational on IP networks, FCC rules also require providers using older forms of network technology to either upgrade their networks to IP or actively work to develop a caller ID authentication solution that is operational on non-IP networks.

ILLEGAL ROBOCALLS AND SPOOFING: The Company is challenged to determine which robocalls are legal versus illegal. The Company is aware that not all robocalls and spoofing are illegal. It is illegal when a caller transmits misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongly obtain anything of value.

Spoofing involves falsifying of caller ID information. It is nefarious when bad actors spoof calls to trick unsuspecting Americans to think the calls are trustworthy because caller ID information appears as if the call came from a neighbor or a familiar or reputable source.

FCC RULE: The Company is required to comply with the following FCC rule:

§64.6305 Robocall mitigation and certification.

(a) Robocall mitigation program requirements. (1) Any voice service provider subject to an extension granted under §64.6304 that has not fully implemented the STIR/SHAKEN authentication framework on its entire network shall implement an appropriate robocall mitigation program as to those portions of its network on which it has not implemented the STIR/SHAKEN authentication framework.

(2) Any robocall mitigation program implemented pursuant to paragraph (a)(1) of this section shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

STIR/SHAKEN AND ROBOCALL MITIGATION PLAN: The Company 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). The Company has the following Robocall Mitigation Plan in effect described below for the non-IP portions:

Robocall Mitigation Policy:

The Company:

1. Will respond to traceback requests from the FCC, civil and criminal law enforcement, and the Consortium in a timely manner in order to ensure that the FCC and law enforcement have information necessary to combat illegal robocalling.
2. Will take steps to mitigate illegal traffic when notified by the Enforcement Bureau.
3. Will take affirmative, effective measures to prevent new and existing customers from making originating illegal robocalls.
4. Will increase business-oriented steps until STIR/SHAKEN can be implemented including investigating with the customer if specific traffic is legitimate or illegitimate.
5. Will increase due diligence related to reviewing call volumes. The Company is aware that knowledge of our customers and due diligence related to call volumes is critical until a STIR/SHAKEN is implemented.
6. Will make every effort, to the best of our abilities, to block a call if it is highly likely to be illegitimate such as:
 - a. The originating telephone number should be network-blocked because it shows up a Do-Not-Originate list or is an unallocated, unused, or invalid number.
 - b. Because reasonable analytics indicated the call is likely malicious in intent. For example, a significant change in a business' originating traffic patterns to suddenly become high volume, very short duration calls might indicate they have been hacked.
7. Has language in the Company's Terms and Conditions to include our Acceptable Use Policy which states: "The provision of voice service by the company assumes that only legitimate calls will be originated or terminated. It is illegal when a caller transmits misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongly obtain anything of value. The company will cooperate with the Federal Communications Commission and law enforcement to provide them information necessary to mitigate illegal traffic."
8. Currently provisions the VCDN table in our Ribbon C15 soft switch for any new phone system customer to only allow provisioned calling numbers in their VCDN table. Any outgoing calls are screened against the VCDN table to ensure they are sending valid outbound caller ID information. Outbound caller ID information that is not in the VDNS

table will be replaced with the main billing number assigned to the PRI or trunks to ensure valid caller ID information is being sent.

9. Has implemented Innovative Systems Terminating Call Manager (TCM) to challenge unwanted calls. This was to offer a solution to our customers to further mitigate unwanted calls. This method challenges incoming calls with a prompt to continue. This method also offers allow and block lists that either we can modify or the customer can modify. This can be applied to any or all trunks or individual lines as deemed necessary. We currently have it available for individual lines.
10. Is not able to go full STIR/SHAKEN at this time as most of our calling trunks between us and our connecting communication companies are TDM. We have implemented Out-of-Band SHAKEN for calls that rely on non-IP technology using a STIR/SHAKEN solution, supplied by TransNexus/ClearIP, to mitigate robocalls on all our TDM trunks and provide a means to monitor call volumes and efficiently respond to any traceback requests.
11. Will continue to follow the best practices for Know Your Customer described by the NANC Call Authentication Trust Anchor Working Group.
(<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

The company utilizes the mitigation technique of “Know Your Customer.” The company is a small, long-established provider that maintains a close relationship with its subscribers and knows its customers. Its customers are generally “mom and pop” users and few of its total customer base have enough call paths to generate the high volume of traffic associated with robocalling allowing us to use targeted in-house analytics to monitor, alert and apprehend suspected robocalling activities.

12. Uses a software solution provided by TransNexus/ClearIP to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls. The software provides detailed reporting identifying suspected illegal robocalls and alerts us if we originate any 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. We immediately investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If we determine that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as appropriate.
13. Has deployed a Ribbon Call History Server, with VQM analytics software by Nex-Tech, to monitor against suspicious calling activities including high call volumes, excessive short duration calling, and high call volumes of non-completed calls. Call monitoring is continuous and automated, and a report of suspected calls is produced daily for review and potential remediation by designated employees.

14. Has registered with the STI-PA from iconectiv and has obtained its own STIR/SHAKEN certificate issued by TransNexus Certification Authority (STI-CA) that is used when authenticating voice traffic that originates and terminates on the IP portions of the company's network that supports SIP calls. A STIR/SHAKEN solution supplied by TransNexus/ClearIP has been implemented on the IP portions of the company's network and will migrate to full STIR/SHAKEN as our upstream provider companies switch the TDM trunks to SIP trunks.

FCC UPLOAD AND CERTIFICATION: The Company will upload and certify per the FCC website which states:

"Welcome to the Robocall Mitigation Database. Pursuant to 47 CFR § 64.6305(b), all voice service providers must file certifications to this Database providing detailed information regarding their implementation of the STIR/SHAKEN caller ID authentication framework and/or a robocall mitigation program.

Through this webpage, members of the public may download voice service providers' certifications. In addition, through the portal found on this webpage, voice service providers may submit their certifications.

You may find an active listing of all voice service providers that have submitted sufficient certifications by clicking View Database below or by downloading the CSV file below. Please note that you may need additional software to view the CSV file.

A voice service provider must possess an FCC Registration Number (FRN) to submit a certification. If you are a voice service provider and would like to submit a certification, and you have an FRN, please click the "Log in" button below. If you wish to submit a certification but do not have an FRN, please click "Create Account" below. After creating an FRN, please return to this page to log in. Full Database submission instructions are available here."²

FCC SUPPORT IF NEEDED: Email FCC staff at RobocallMitigationDatabase@FCC.gov."

² https://fccprod.servicenowservices.com/rmd?id=rmd_welcome