

Robocall Mitigation Plan

Colo Telephone Company

Executive Summary

The purpose of this Robocall Mitigation Plan (RMP) is to implement best practices, procedures and policies to mitigate or reduce originating illegal traffic (aka robocalls).

Colo Telephone Company (Colo) will:

1. Know its customer and will follow the best practices for vetting caller identity as described in the NANC Call Authentication Trust Anchor Working Group as listed below:
 - a. <https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>
2. Cooperate with traceback requests received from carriers, the registered traceback consortium and law enforcement within 24 hours of receipt of such request
3. Take steps when notified by the Commission's Enforcement Bureau to mitigate any suspected illegal traffic
 - a. Investigate suspected illegal traffic
 - b. Report back to the Enforcement Bureau the results of said investigation and any mitigation steps taken
 - i. Including whether any of the calls came from another voice service provider with direct access to the U.S. public switched telephone network (PSTN)
4. Prevent any calls being blocked to or from emergency services
5. Implement the following best practices, policies and procedures as part of Colo's RMP

Point of contact for this RMP:

Primary Contact: Shane Bellon
Title: General Manager
Address: 303 Main Street, P.O. Box 315, Colo, IA 50056
Phone: 641-377-2202
Email: shane@colotel.org

Regulatory Background

The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) requires voice service providers to implement STIR/SHAKEN authentication on SIP/IP traffic on their networks as well as to implement an RMP on non-SIP/IP traffic (aka TDM traffic) on their network.

The FCC granted a continuing extension for voice service providers with non-IP networks (aka TDM) from implementing STIR/SHAKEN authentication. Below are the rule sections that apply to Colo:

§ 64.6304 Extension of implementation deadline.

(a) ***Small voice service providers.***

(2) For purposes of this [paragraph \(a\)](#), “small voice service provider” means a provider that has 100,000 or fewer voice service subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the provider's affiliates).

(d) ***Non-IP Networks.*** Those portions of a voice service provider or gateway provider's network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP calls are deemed subject to a continuing extension. A voice service provider subject to the foregoing extension shall comply with the requirements of [§ 64.6303\(a\)](#) as to the portion of its network subject to the extension, and a gateway provider subject to the foregoing extension shall comply with the requirements of [§ 64.6303\(b\)](#) as to the portion of its network subject to the extension.

§ 64.6303 Caller ID authentication in non-IP networks.

(a) Except as provided in [§§ 64.6304](#) and [64.6306](#), not later than June 30, 2021, a voice service provider shall either:

(1) Upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework as required in [§ 64.6301](#) throughout its network; or

(2) Maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or actively testing such a solution.

Basis for Exemption

Colo is a “small voice service provider” that has approximately 295 voice service subscriber lines aggregated over all of the company’s affiliates. Colo’s voice network is currently non-IP for all outgoing traffic to the tandem and therefore qualifies for the exemption. Colo is required to comply with the requirements of §64.6303 (a). This non-IP tandem connection carries all traffic to the outside world and relies on a technology that cannot originate, carry, process, or terminate SIP calls.

Meeting §64.6303(a)(2) Obligations

Colo is a member of NTCA and the National Exchange Carrier Association (NECA) which act as its third party representatives to develop a non-internet Protocol caller identification authentication solution. NTCA and NECA are members of the ATIS Non-IP Call Authentication Task Force which developed the non-IP call authentication solutions.

Roll in the Call Chain

Colo is a voice service provider providing voice service and broadband services to end user customers inside its regulated serving area. Colo does not have a STIR/SHAKEN obligation at this time due to having a non-IP network (see above).

Operating Company Number (OCN)

Colo’s Operating Company Number (OCN) is 1134.

Status of participation in the Robocall Mitigation Database (RMD)

Colo has not been prohibited from filing in the RMD.

Commission, law enforcement and/or regulatory action or investigation related to spoofing or suspected unlawful robocalls

Colo has not been involved in any Commission, law enforcement and/or regulatory action related to spoofing or suspected unlawful robocalls. Colo has not been removed from the RMD and precluded from refiling due to deficiencies needing to be cured. Colo authorization has not been revoked due to continuing violations of the Commission’s robocall mitigation rules.

Prior two years status

In the past two years Colo has not been the subject of a formal Commission, law enforcement and/or regulatory action or investigation with accompanying findings of actual or suspected wrongdoing due to Colo transmitting, encouraging, assisting or otherwise facilitating illegal robocalls or spoofing related to spoofing or suspected unlawful robocalls.

Know your upstream provider

Colo receives the majority of its traffic from Aureon, a Centralized Equal Access provider in Iowa. Aureon blocks traffic from carriers that are not in the RMD or have been removed from the RMD.

Know your Customer

Colo takes the following steps to prevent new and existing customers from originating robocalls over its network:

- The vast majority of Colo’s subscribers are defined as a “direct” retail consumer or commercial end users located inside its serving areas
 - These subscribers are best defined as residential and small business customers and Colo will:
 - Validates the residential or business customer’s identity
 - Validates the physical location which will be the fixed location where service is established
- Colo has no commercial VoIP customers. If Colo obtains one or more, Colo will gather the following information as reasonably practical to “Know your Customer”:
 - Physical business location
 - Contact person’s information
 - State or country of incorporation
 - Federal tax ID number
 - Nature of the customer’s business
- Colo does not offer service currently to wholesale subscribers

Robocall Mitigation Plan (RMP)

Robocall Mitigation Efforts: Long Distance Traffic

Colo uses a third party administrator, Aureon, for call analytics systems used to identify and block illegal traffic. Aureon, an end-to-end technology solutions organization, provides a Caller Identification Authentication (CIDA) service which includes Outbound Shield technology. This Outbound Shield uses a curated list of high-risk phone numbers and detects invalid numbers. If the calling number has been reported as spam, the calling number will be prevented from completing outbound calls.

See Appendix A for a copy of the certification by Colo for Aureon's CIDA service.

Additionally, Colo has implemented the following best practices, policies and procedures to mitigate unlawful illegal traffic (robocalls):

- Know its customer and will follow the best practices for vetting caller identity as described in the NANC Call Authentication Trust Anchor Working Group as listed below:
 - <https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>
- Cooperate with traceback requests received from carriers, the registered traceback consortium and law enforcement within 24 hours of receipt of such request
- Take steps when notified by the Commission's Enforcement Bureau to mitigate any suspected illegal traffic
- Investigate suspected illegal traffic
 - Report back to the Enforcement Bureau the results of said investigation and any mitigation steps taken
 - Including whether any of the calls came from another voice service provider with direct access to the U.S. public switched telephone network (PSTN)
- Prevent any calls being blocked to or from emergency services

Robocall Mitigation Plan (RMP)

Robocall Mitigation Efforts: Local and/or EAS Traffic

Colo has implemented the following best practices, policies and procedures to mitigate unlawful illegal traffic (robocalls):

- Know its customer and will follow the best practices for vetting caller identity as described in the NANC Call Authentication Trust Anchor Working Group as listed below:
 - <https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>
- Cooperate with traceback requests received from carriers, the registered traceback consortium and law enforcement within 24 hours of receipt of such request
- Take steps when notified by the Commission's Enforcement Bureau to mitigate any suspected illegal traffic
- Investigate suspected illegal traffic
 - Report back to the Enforcement Bureau the results of said investigation and any mitigation steps taken
 - Including whether any of the calls came from another voice service provider with direct access to the U.S. public switched telephone network (PSTN)
- Prevent any calls being blocked to or from emergency services
- Nearly all residential and business lines can place only one call at a time
- All residential and business lines are only able to place calls originating from their own phone number
- Only numbers residing in our switch are assigned to residential and business lines
- Investigate any complaints about legitimate calls being blocked

Appendix A Third Party Service Agreements



7760 Office Plaza Drive South
West Des Moines, Iowa 50266

*The following documentation is to serve as proof of Colo Telephone Company
(Company Name) robocall mitigation efforts in compliance with the Traced Act.*

Robocall Mitigation Efforts: Long Distance Traffic

Aureon, an end-to-end technology solutions organization, provides a Caller Identification Authentication (CIDA) service which includes Outbound Shield technology. This Outbound Shield uses a curated list of high-risk phone numbers and detects invalid numbers. If the calling number has been reported as spam, the calling number will be prevented from completing outbound calls.

I, Larry W. Springer (name), verify that Colo Telephone Company (Company Name) utilizes the aforementioned Caller Identification Authentication (CIDA) service to mitigate unlawful robocalling for long distance traffic.

Date: 6/21/2021

Robocall Mitigation Efforts: Local Traffic

I, _____ (name), verify that _____ (Company Name) utilizes the below robocall mitigation efforts for local traffic.

Description of robocall mitigation efforts in place:

Date: _____

TALENT • TECHNOLOGY • TOOLS

Certification of Robocall Mitigation Plan by Officer of the Company

I, , certify that the above information is true and correct to the best of my knowledge. My title is, General Manager CISO, and am an officer of the company.