

STIR/SHAKEN Implementation and Robocall Mitigation Plan

Reynolds Cable, Inc. (d/b/a Reynolds Communications)

Executive Summary

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

Reynolds Cable, Inc. (Reynolds) 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 Reynolds's RMP

Point of contact for this RMP:

Primary Contact: Jace A. Taylor
Title: General Manager / C.O.O
Address: 221 W Main Street, PO Box 27, Reynolds, IL 61279
Phone: 309-372-4214
Email: jataylor@reytel.net

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.

Inteliquent provides STIR/SHAKEN services on behalf of Reynolds consistent with 47 CFR § 64.6301(a).

Roll in the Call Chain

Reynolds is a marketing and billing collection agent of voice services and provides broadband services to end user customers inside its serving area. Reynolds does not have control over the traffic and is only a marketing and billing collection agent. To the best of Reynolds' knowledge, STIR/SHAKEN is provided on this traffic by Inteliquent.

Operating Company Number (OCN)

Reynolds' does not have an Operating Company Number (OCN).

Status of participation in the Robocall Mitigation Database (RMD)

Reynolds 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

Reynolds has not been involved in any Commission, law enforcement and/or regulatory action related to spoofing or suspected unlawful robocalls. Reynolds has not been removed from the RMD and precluded from refiling due to deficiencies needing to be cured. Reynolds 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 Reynolds 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 Reynolds transmitting, encouraging, assisting or otherwise facilitating illegal robocalls or spoofing. related to spoofing or suspected unlawful robocalls.

Know your upstream provider

Reynolds does not have control over the traffic, but to the best of Reynolds' knowledge Inteliquent verifies that all carriers in which it receives traffic are listed in the RMD.

Know your Customer

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

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

Robocall Mitigation Plan (RMP)

Robocall Mitigation Efforts: Long Distance Traffic

Reynolds is a marketing and billing collection agent on behalf of Inteliquent, and to the best of Reynolds' knowledge Inteliquent provides STIR/SHAKEN consistent with 47 CFR § 64.6301(a) for all traffic consistent with 47 CFR § 64.6301(a). Inteliquent is a communications enabler offering network-based voice and messaging services to wireless, cable, carriers and communication service providers.

Additionally, Reynolds 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

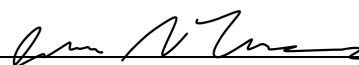
Reynolds has implemented the following best practices, policies and procedures to mitigate unlawful illegal traffic (robocalls):

- 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)

Appendix A Third Party Service Agreements

None

Certification of Partial STIR/SHAKEN Implementation and 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, Chief Operating Officer, and am an officer of the company.