

Partial STIR/SHAKEN Implementation and Robocall Mitigation Plan

**Dell Telephone Cooperative
Delcom Broadband**

Executive Summary

The purpose of this Partial 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).

Dell Telephone Cooperative and Delcom Broadband (Dell) 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 Dell's RMP

Point of contact for this RMP:

Primary Contact: Grant Spence
Title: General Manager
Address: 610 South Main St., P.O. Box 67, Dell City, TX 79837
Phone: 915-964-2352
Email: grant@delltelco.com

Secondary Contact: Luis Guillen
Title: Network Operations Manager
Address: 610 South Main St., P.O. Box 67, Dell City, TX 79837
Phone: 915-964-2352
Email: Luis@delltelco.com

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 Dell:

§ 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

Dell is a “small voice service provider” that has approximately 1,065 voice service subscriber lines aggregated over all of the company’s affiliates. Dell’s voice network is currently partial IP and partial non-IP for all outgoing traffic to the tandem and therefore qualifies for the exemption.

For the non-IP portion of its network, Dell is required to comply with the requirements of §64.6303 (a). This non-IP tandem connection carries some of their traffic to the outside world and relies on a technology that cannot originate, carry, process, or terminate SIP calls.

Inteliquent, Inc., provides STIR/SHAKEN services on behalf of Dell. For customers that are assigned to certain trunk groups, outgoing long distance calls are STIR/SHAKEN. Customers not on those select trunk groups remain on TDM and are subject to Robocall Mitigation efforts.

Meeting §64.6303(a)(2) Obligations

Dell is a member of the 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

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

Operating Company Number (OCN)

Dell’s Operating Company Number (OCN) are 2066 and 783G (Delcom Broadband).

Status of participation in the Robocall Mitigation Database (RMD)

Dell 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

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

Know your upstream provider

N-Com, A JSI Company, an engineering service company, provides a Robocall Mitigation detection service on originating calls. N-Com, A JSI Company downloads call detail records (CDR's) monthly, runs them through a proprietary program that detects unusual high originating call volume and provides a report identifying lines, if any, that are detected.

Know your Customer

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

- The vast majority of Dell'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 Dell will:
 - Validates the residential or business customer's identity
 - Validates the physical location which will be the fixed location where service is established
- Dell has no Commercial VoIP customers. If Dell obtains one or more, Dell 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
- Dell does not offer service currently to wholesale subscribers

Robocall Mitigation Plan (RMP)

Robocall Mitigation Efforts: Long Distance Traffic

Dell uses a third party administrator, N-Com, A JSI Company, for call analytics systems used to identify and block illegal traffic. N-Com, A JSI Company, an engineering service company, provides a Robocall Mitigation detection service on originating calls. N-Com, A JSI Company downloads call detail records (CDRs) monthly, runs them through a proprietary program that detects unusual high originating call volume and provides a report identifying lines, if any, that are detected.

Dell uses a third party administrator, Inteliquent, Inc., for STIR/SHAKEN. Inteliquent, Inc., an end-to-end technology solutions organization, provides STIR/SHAKEN service.

Additionally, Dell 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

Robocall Mitigation Plan (RMP)

Robocall Mitigation Efforts: Local and/or EAS Traffic

Dell 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

Dell has contracted with N-Com, A JSI Company to provide Dell Robocall Mitigation detection services

Dell has contracted with Inteliquent, Inc. to provide STIR/SHAKEN services

STIR / SHAKEN Attestation and Verification Service Schedule

This **STIR/SHAKEN Attestation and Verification Service Schedule** (this "Service Schedule") is made between **Dell Telephone Cooperative, Inc.** ("Customer") and **Inteliquent, Inc.** ("Carrier"). This Service Schedule is made under the terms of the Master Services Agreement between Customer and Carrier (as amended, the "MSA"). If Onvoy, LLC is the providing party under the MSA, then Inteliquent, Inc. is signing this Service Schedule on behalf of Onvoy, LLC.

Under the MSA and this Service Schedule, Customer will receive, and Carrier will provide, the Services (as defined below). In the event of a conflict between a term in this Service Schedule and a term in the MSA, the term in this Service Schedule will govern with respect to the Services. The definitions in the MSA apply to any term that is used but not defined herein. This Service Schedule is effective on March 13, 2024 ("Effective Date").

1. Definitions.

- 1.1. **Attestation:** An indication populated in the SHAKEN PASSporT of the extent to which the originating Service Provider has identified and authenticated a calling party originating the call and determined there is an association between the calling party and the calling TN.
- 1.2. **Certificate:** A digital profile that contains the Public Key and proves ownership of the call for the Service Provider. The Certificate is provided by an authorized Certification Authority.
- 1.3. **Certification Authority:** An approved entity that issues and governs digital certificates used to authenticate the calling party.
- 1.4. **Identity Headers:** A SIP header containing a SHAKEN PASSporT as specified in the STIR/SHAKEN specifications.
- 1.5. **PASSporT:** Inserted into an Identity Header and contains information regarding the originating call such as attestation, calling TN, and information about the originating calling entity.
- 1.6. **Public Key:** Used by terminating Service Provider to verify validity of originating Secure Private Key.

- 1.7. **Verstat:** Information derived from originating Service Provider Attestation which will indicate, TN-Validation-Passed, TN-Validation-Failed or No-TN-Validation.
- 1.8. **Secure Private Key:** Used by originating Service Provider to sign calls and is stored in a secure key store.
- 1.9. **Service Provider:** An entity that provides voice services to end users, and that meets the requirements established by the STI-GA, STI-PA, and Certificate Authority to obtain call signing credentials.
- 1.10. **SHAKEN:** Signature based handling of asserted information using tokens.
- 1.11. **STI-GA:** Secure Telephone Identity Governance Authority, which is the entity that defines the rules governing the certificate management infrastructure to ensure effective use and security of Certificates.
- 1.12. **STI-PA:** Secure Telephone Identity Policy Administrator, which is the entity that has been chosen by the STI-GA to implement the rules of the STI-GA. iconectiv is currently the STI-PA.
- 1.13. **STIR:** Secure Telephone Identity Revisited.
- 1.14. **TN:** Telephone Number.

2. Authentication Services. Carrier will provide SHAKEN Authentication Services (collectively, the "Services") to Customer as described below. For Services to be provided under this Service Schedule, calls must be sent to Carrier in E.164 format.

2.1. Hosted Authentication. Carrier will host Customer's Service Provider Certificate, Secure Private and Public Keys. Carrier and Customer will work together to determine proper Attestation level based on current industry rules and requirements for Customer's calls. Carrier will generate signed Identity Header and insert Customer's SIP Invites.

- (i) Customer will work with a third-party Certificate Authority to host Customer's Public Certificate Repository.
- (ii) Carrier will maintain Customer's Secure Private Key used for signing on a secure platform.
- (iii) Signed Identity Headers will only be passed over other SIP Service Provider connections.

Notwithstanding any other provision, if the parties are unable to agree on the proper attestation, Carrier may terminate the Service immediately. Moreover, Customer will indemnify Carrier for any liability arising from a third-party claiming that the attestation level is improper.

2.2 Authentication Call Hand Back Service. Customer may have Carrier sign calls and send the calls back to the Customer network for further routing from the Customer. This Service will require a separate trunk group for routing calls between Carrier and Customer.

2.4. Out of Band Authentication. Upon industry wide adoption of an Out of Band solution for TDM networks, Carrier will provide such service.

3. **Verification Services.** Carrier will provide SHAKEN Verification Services to Customer as outlined below.

3.1. **Verstat.** Carrier will send the Verstat to Customer on any inbound call with a signed Identity Header. The Verstat value will be generated based on the Verification Services determination on the TN validation. Verstat applied per inbound trunk group, and Carrier and Customer to jointly determine applicable trunk groups.

4. **Limitations.** Carrier makes no assertions that all inbound or outbound calls will pass proper signed Identity Headers to or from other Service Providers. Limitations to the STIR/SHAKEN ecosystem exists, such as TDM connectivity and Service Provider implementation, which will cause failure of transporting the signed Identity Headers to or from other carriers. Carrier cannot guarantee that other carriers will sign calls with the proper Attestation or will correctly interpret signed Identity Headers from Service Provider.

5. **Term.** The term of this Service Schedule will begin on the Effective Date and expire after one year. The term of this Service Schedule will automatically renew for annual periods unless either party provides written notice to the other party at least 90 days prior to the end of the initial term or any renewal period.

6. **Limitation of Liability.** IF CARRIER IS EVER HELD LIABLE IN RELATION TO THIS SERVICE SCHEDULE AND WHETHER THE CLAIM IS UNDER CONTRACT, LAW OR ANY OTHER THEORY OF LIABILITY, CARRIER'S LIABILITY UNDER THIS SERVICE SCHEDULE IS LIMITED TO PROVEN DIRECT DAMAGES AND WILL NOT EXCEED THE LESSER OF (i) THE TOTAL AMOUNT PAID TO CARRIER FOR THE THREE MONTHS PRIOR TO THE EVENT OR EVENTS IN QUESTION OR (ii) \$5,000.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement as of the Effective Date.

Dell Telephone Cooperative, Inc.

Inteliquent, Inc.



Certification of Partial STIR/SHAKEN Implementation and Robocall Mitigation Plan by Officer of the
Company

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