

Robocall Mitigation Plan

Meriplex Telecom LLC

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).

Meriplex Telecom LLC (Meriplex) 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 Meriplex's RMP

Point of contact for this RMP:

Primary Contact: Chris DeFortuna
Title: Director Cloud & Core
Address: 10111 Richmond Ave, Houston, TX 77042
Phone: 281-404-2297
Email: chris.defortuna@meriplex.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.

TransNexus?? provides STIR/SHAKEN services on behalf of Meriplex consistent with 47 CFR § 64.6301(a).

Roll in the Call Chain

Meriplex is a voice service provider providing voice service and provides broadband services to end user customers inside its serving areas.

Operating Company Number (OCN)

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

Status of participation in the Robocall Mitigation Database (RMD)

Meriplex 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

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

Know your upstream provider

Meriplex verifies that all carriers in which it receives traffic are listed in the RMD.

Know your Customer

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

- The majority of Meriplex subscribers are defined as a “direct” 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
- Meriplex has Commercial VoIP customers. Meriplex will gather the following information as reasonably practical to “Know your Customer”:
 - Physical business location
 - Contact person’s information
 - Federal tax ID number
 - State or country of incorporation
- Meriplex does or does not offer service currently to wholesale subscribers

Robocall Mitigation Plan (RMP)

Robocall Mitigation Efforts: Long Distance Traffic

Meriplex provides STIR/SHAKEN through an agreement with TransNexus consistent with 47 CFR § 64.6301(a) for all of the traffic consistent with 47 CFR § 64.6301(a). ? is a communications enabler offering network-based voice and messaging services to wireless, cable, carriers and communication service providers. .

Please see Appendix A for information on the agreement with TransNexus.

Additionally, Meriplex 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

Meriplex 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
- 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
- Businesses with Trunk Hunting are allowed to send spoofed numbers for legitimate business needs. This includes a main line number, DODs, toll free number, etc.
 - Caller ID and Setup are reviewed when the service is installed to verify legitimate caller ID information
- Only numbers residing in our switch are assigned to residential and business lines
- Investigate any complaints about legitimate calls being blocked
- Call Detail Records (CDRs) are created for all long distance and EAS calls and are searchable

Appendix A Third Party Service Agreements

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, _____, and am an officer of the company.