



Tri-County Telephone Company, LLC - d/b/a Ritter Communications Robocall Mitigation Plan (RMP)

Service Definition

All voice traffic origination on the network, including interconnected VoIP service, as defined in 47 CFR § 64.6300(n)(1), is subject to the robocall mitigation program described herein.

Scope & Zero Tolerance Policy

Tri- County Telephone Company, LLC (Ritter) provides telephone service and applies this Robocall Mitigation Program to all originating, transiting, and gateway traffic, whether retail or wholesale. The Company maintains a zero-tolerance policy for illegal robocalling, caller ID spoofing, traffic pumping, and consent violations. Any customer or upstream provider associated with suspected illegal activity is subject to immediate mitigation measures, up to and including termination.

Know Your Customer

Ritter does not knowingly provide service to entities engaged in auto warranty campaigns, debt relief or credit repair mass dialing, lead resale operations, or government impersonation. Furthermore, Ritter does not knowingly provide interconnected VoIP service to customers unwilling to provide campaign-level documentation or resellers lacking downstream customer transparency.

Prior to activation, Ritter requires:

- Articles of Incorporation, or equivalent formation documents
- Government-issued identification of responsible officer
- Beneficial ownership disclosure
- Campaign description and sample call scripts
- Evidence of consent collection procedures
- TCPA compliance policy
- Dialing platform identification (including vendor and technical configuration)
- Proof of number authorization (LOA or assignment verification)

Ritter conducts thorough vetting of all interconnected VoIP customers, including verifying business legitimacy, physical address, and intended traffic description to prevent the origination of illegal robocalls. High-volume, or outbound centric customers (high-risk customers) are subject to executive compliance committee approval, call sample review, proof-of-consent audit capability, traffic volume caps during initial 30–60 days, and a financial security deposit. Additional detail of the best practices that Ritter employs can be found at the following link: <https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf>

Traceback Commitment:

Ritter responds to all traceback requests within 24 hours, prioritizing traceback notices from:

- The Industry Traceback Group
- State Attorneys General
- Federal enforcement agencies

Ritter cooperates fully with enforcement investigations. Any traffic confirmed to be illegal will be immediately blocked. Confirmed illegal robocall originators are permanently barred from re-onboarding.

STIR/SHAKEN Implementation Status

Mandatory STIR/SHAKEN Authentication Controls

Ritter has introduced the STIR/SHAKEN authentication framework to a segment of its network. Ritter has various IP Interconnections with Sinch, formerly known as Inteliquent, who is our upstream provider for long distance traffic. By implementing TNSI-Metaswitch Stir/Shaken product, Ritter can attest that calls originating its network and traversing these interconnections adhere to the requirements outlined in 47 CFR § 64.6301(a)(1) and (2).

Ritter is subject to the ongoing extension provided by 47 CFR § 64.6304 (d) for the implementation of STIR-SHAKEN. This provision exempts certain portions of the voice service provider's network from STIR-SHAKEN Caller ID Authentication. These exemptions pertain to segments of our network that rely on old transport and/or upstream provider equipment that is not capable of originate or terminate interconnected VOIP calls end to end in the setup process.

Ritter operates in several rural markets that rely on non-IP interconnections to market Tandems and/or various carriers to complete local and regional calls. Until upstream providers that Ritter exchanges traffic within these markets update their facilities or allow for IP Interconnections, Ritter will continue to monitor progress on out-of-band Stir-Shaken and will adhere to any FCC mandates that may come to realization in the future. **Therefore, as of 5/19/2023 Tri-County Telephone Company, LLC voice traffic is partially attested.**

Monitoring & Enforcement

Ritter is a voice service provider offering a variety of voice calling services. Its customers generally do not originate high volume calls and Ritter has not received information suggesting that robocalls are originated on its network. Therefore, Ritter does not consider its network at high risk of originating illegal robocalls.

Ritter uses [TNS Call Guardian](#) analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination activity. If Ritter has a reasonable basis to believe that a customer is originating illegal robocalls, it will require the customer to remedy the problem and, if effective action is not taken, Ritter can suspend and/or terminate service to the customer.

What is Call Guardian Authentication Hub?

Call Guardian Authentication Hub (CGAH) is a hosted, managed service provided by Metaswitch in conjunction with our partner Transaction Network Services (TNS). It combines two industry leading products with complementary technologies:

- **Call blocking and filtering analytics** from the TNS Call Guardian product, to provide protection of your subscribers from unwanted calls, whether they be robocalls, spam, nuisance, fraudulent calls, political campaigns, charities, telemarketers, etc.
- **Call signing and verification** from the **Metaswitch QCall STIR/SHAKEN** product.

By using CGAH, Ritter actively blocks calls originating from invalid numbers, calls from do not originate (DNO) lists and blocking any calls matching reputation scores of a -3 or -4 via TNS scoring.

Numbering Governance and Anti-Spoofing Controls

Caller ID must correspond to numbers assigned by the Company and authorized via documented LOA. Random, invalid, or unallocated numbering is blocked at origination. Dynamic caller ID manipulation is prohibited unless pre-approved. Customers are prohibited from rotating large number pools to evade analytics.

Ongoing Compliance Oversight

Ritter maintains:

- A designated Robocall Mitigation Officer
- Quarterly internal compliance audits
- Annual executive review of mitigation performance
- Written escalation procedures
- Employee training specific to illegal robocall detection

Record Retention and Audit Readiness

Ritter retains for no less than five (5) years:

- Customer onboarding documentation
- Attestation assignment logs
- Traffic analytics reports
- Traceback correspondence
- Mitigation action records

Records are maintained in a sufficient manner to demonstrate compliance to regulators upon request

Robocall Mitigation Database Certification

Ritter certifies in the FCC Robocall Mitigation Database that:

- It has fully implemented STIR/SHAKEN for all IP-originated interconnected VoIP traffic.
- It has implemented this enhanced mitigation program for any non-IP or unsigned traffic.
- It conducts active monitoring and enforces zero-tolerance policies.
- It will update its certification promptly upon any material change.

Principles, Affiliates, Subsidiaries, and Parent Companies

Company Name	Relationship to Filing Entity	Type of Company	% Owned by Filing Entity	Management or Control of Entity
E. Ritter Communications Holdings, LLC	Parent	Holding Co.	100%	Heath Simpson – CEO & Managing Control
E. Ritter Telephone Company, LLC	Subsidiary	ILEC	0%	Heath Simpson – CEO & Managing Control
Tri-County Telephone Company, LLC	Subsidiary	ILEC	0%	Heath Simpson – CEO & Managing Control
Millington Telephone Company, LLC	Subsidiary	ILEC	0%	Heath Simpson – CEO & Managing Control
MTel Long Distance, LLC	Subsidiary	ILEC	0%	Heath Simpson – CEO & Managing Control
E. Ritter Communications, LLC	Subsidiary	CLEC/IPES	0%	Heath Simpson – CEO & Managing Control