

Clay County Rural Telephone Cooperative, Inc. DbA Endeavor Communications

Robocall Mitigation Plan (Rev. 2026)

Provider Type: Originating Voice Service Provider

Effective Date: March 2nd, 2026

Legal Company Name: Clay County Rural Telephone Cooperative, Inc. DbA Endeavor Communications.

FCC Registration Number (FRN): 0004970711

Robocall Mitigation Database Filing ID: RMD0004337

Primary Compliance Contact:

Name: Thomas Forajter

Title: VP of GigTel Operations

Phone: (765) 795-9206

Email: Thomas.Forajter@GigTel.com

1. Executive Summary & Certification

This Robocall Mitigation Plan describes the specific policies, procedures, technical controls, and monitoring systems implemented by Endeavor Communications, under the brand of GigTel, as an Originating Voice Service Provider operating its own switching infrastructure. Endeavor Communications originates traffic directly from end users and business customers and is responsible for applying caller authentication, monitoring, and mitigation controls at the network origination point.

Endeavor Communications and GigTel certify that they have implemented reasonable steps to prevent the origination of illegal robocalls and will comply with all applicable FCC robocall mitigation obligations.

2. Network Architecture & Origination Control

Endeavor Communications operates its own softswitch infrastructure and directly provisions customers. All outbound traffic originates from Endeavor-controlled SBCs, servers, or switching equipment, or from another trusted white-label reseller's network that has also submitted its own Robocall Mitigation Plan.

Origination controls are applied at the SIP authentication layer and enforced prior to call routing to upstream carriers or interconnection partners.

3. STIR/SHAKEN Implementation

Endeavor Communications fully implements STIR/SHAKEN authentication for all IP-originated traffic in accordance with FCC requirements.

As the originating provider, Endeavor Communications signs outbound calls using authorized certificates issued by the STI Governance Authority.

Attestation Policy:

- A-level attestation is assigned only when Endeavor Communications has a direct authenticated relationship with the end user and can verify the right to use the calling number.
- B-level attestation is applied when the customer is known, but the number control cannot be fully verified.
- C-level attestation is used when calls are originated on behalf of another provider or reseller without direct number control validation.

4. Know Your Customer (KYC) Controls

Prior to service activation, Endeavor Communications conducts risk-based due diligence on all customers. This KYC procedure includes:

- Verification of legal entity registration and EIN
- Validation of physical business address
- Confirmation of authorized business representatives
- Review of intended call use case and volumes
- Screening against enforcement databases and known bad-actor lists
- Customer agreements include descriptions and links to GigTel's online privacy policy, which explicitly covers prohibited uses of the systems and features.

5. Traffic Monitoring & Analytics

Endeavor Communications continuously monitors outbound traffic across its switching infrastructure. These monitoring controls include:

- Real-time call detail record (CDR) analysis
- Short-duration call ratio thresholds
- High call attempt rate detection
- Burst traffic alerts
- ANI spoofing pattern detection
- Do Not Originate (DNO) enforcement
- Defined traffic thresholds trigger automated alerts and internal investigation workflows.

6. Mitigation & Enforcement Actions

When suspicious or unlawful traffic is detected, GigTel initiates an investigation within 24 hours. Mitigation steps may include:

- Immediate rate limiting or temporary service suspension
- Customer notification and compliance review
- Permanent service termination for confirmed violations
- Reporting to upstream carriers as required

7. Traceback & Regulatory Cooperation

GigTel responds to all traceback requests from the FCC, law enforcement, and authorized industry traceback consortiums within 24 hours. Relevant CDRs, routing information, and customer identification data are retained and provided in accordance with regulatory requirements.

8. Record Retention & Internal Audit

- Minimum CDR retention period of 18 months, with additional retention of 36 to 60 months for special use cases, as required
- Documentation of investigations and enforcement actions
- Quarterly internal review of mitigation thresholds
- Annual executive review of robocall mitigation effectiveness

9. Change Management & Annual Recertification

Material changes to this plan or Endeavor Communications contact information will be updated in the FCC Robocall Mitigation Database within 10 business days.

Endeavor Communications completes annual recertification of its Robocall Mitigation Database filing in accordance with FCC deadlines.