



BICENTEL, LLC

Robocall Mitigation Plan

Background and Regulatory Status

Bicentel, LLC is an international wholesale telecommunications provider serving U.S. and foreign carriers. The Company operates primarily as an intermediate provider and does not originate end-user consumer traffic. The Company does not knowingly originate or knowingly facilitate illegal robocall traffic. The Company takes reasonable and effective steps to prevent the origination, transmission, and processing of illegal robocalls affecting traffic routed to or from the United States telecommunications network.

This plan is designed to demonstrate reasonable mitigation efforts.

STIR/SHAKEN Implementation

As applicable under 47 CFR § 64.6304, the Company has implemented STIR/SHAKEN authentication and validation for SIP-based traffic traversing its IP network. The Company monitors attestation integrity and may block traffic with improper or invalid attestation where required.

The Company:

- Validates incoming attestation levels (A, B, and C)
- Monitors traffic patterns associated with downgraded or anomalous attestations
- Investigates repeated or improper use of full (A-level) attestation
- Blocks or restricts traffic where attestation appears fraudulent, improper, or absent without justification

Improper or misleading attestation is treated as a material compliance violation and may result in immediate suspension of the originating provider.

Robocall Risk Management Framework

The Company applies a risk-based mitigation approach including:

- Customer onboarding risk scoring
- Traffic pattern profiling
- Continuous anomaly detection
- Escalation thresholds



Risk Classification

Risk Level	Description
Low	Established wholesale carriers with clean compliance history and stable traffic patterns.
Medium	Providers with moderate traffic variability or higher call volume campaigns requiring closer supervision.
High	Providers or traffic patterns presenting elevated risk indicators associated with potential robocall activity.
Prohibited	Traffic or customers confirmed or reasonably suspected of illegal robocall activity or regulatory non-compliance.

High-risk classifications include:

- Auto-dialer service providers
- Political campaign traffic
- Short-duration call campaigns
- International gateway arbitrage traffic

Know Your Customer (KYC)

Bicentel conducts reasonable due diligence on its wholesale customers to understand the nature of their business and mitigate the risk of unlawful robocalling activity.

Customers are contractually required to comply with all applicable federal and state laws regarding robocalling and caller ID authentication.

Traffic Monitoring & Analytics

The Company maintains real-time automated monitoring systems including:

- CPS thresholds
- Short-duration ratio controls
- Burst traffic detection
- Invalid/unallocated number detection
- Spoofing detection
- ASR anomaly alerts

External sources include:

- Industry Traceback Group (ITG) notifications
- FCC Enforcement Bureau advisories
- Carrier complaint exchanges



Immediate Mitigation & Escalation

Upon detection of suspicious traffic:

- Compliance review initiated within 2 hours
- Customer notification
- Traffic rate-limiting or blocking

If illegal traffic is confirmed:

- Immediate suspension
- Reporting to regulators when required

Traceback Commitment

The Company commits to:

- Respond within 24 hours to authorized traceback requests
- Provide complete CDRs and SIP headers where applicable
- Identify immediate upstream source
- Preserve investigative evidence
- Cooperate fully with ITG, FCC, and law enforcement

The Company maintains designated compliance and network operations personnel responsible for coordinating traceback responses. Roles and responsibilities are documented internally, and escalation procedures ensure timely resolution of suspicious traffic or enforcement requests.

Record Retention

Records are retained for a minimum of two (2) years and may be retained up to five (5) years for regulatory defense and investigation support.

Internal Controls, Audit, and Documentation

The Company maintains formal internal compliance controls including:

- Customer due diligence files
- Call Detail Record (CDR) archives
- Traceback logs and investigation records
- Regulatory reporting documentation
- Executive compliance review summaries



An internal compliance review is conducted on a periodic basis, including traffic analysis and mitigation effectiveness assessment.

Compliance Training Program

The Company maintains an internal robocall compliance training program that includes:

- Mandatory compliance training for relevant personnel
- Specialized training for NOC and compliance staff
- Periodic updates reflecting regulatory changes
- Executive-level compliance briefings

Program Review and Updates

This Plan is reviewed:

- Annually
- Following FCC rule changes
- Following enforcement inquiries

The Company will update its RMD certification within 10 business days of any material change.

Bicentel, LLC reserves the right to modify, add, delete, or otherwise amend any of the policies and procedures described in this Plan at any time, as it deems necessary or appropriate to reflect changes in its business, capabilities, or operational requirements.