

IMPORTANT NOTICE: As of 03/01/2026, this Robocall Mitigation Plan (RMP) has been formally updated to include enhanced mitigation controls. See March 1, 2026 Addendum included herein.

Robocall Mitigation Plan 01/01/2025

Submitted by: Signal Edge Telecom LLC

Address: 500 S. Australian Avenue, Ste 600 #1083, West Palm Beach, FL 33401

Compliance Director: Karen Ferro

Phone: (850) 820-3263

Email: Karen@signaledgetelecom.com

Approved by: Karen Ferro, Compliance Manager

Submitted in accordance with 47 C.F.R. § 64.6305

Executive Summary

Signal Edge Telecom LLC ("Signal Edge") submits this Robocall Mitigation Plan (RMP) in compliance with 47 C.F.R. § 64.6305. As a voice service provider, Signal Edge is committed to a comprehensive and proactive strategy to mitigate illegal robocalls across its network. We prioritize industry compliance, customer trust, and technological leadership to maintain the integrity of our services.

I. STIR/SHAKEN Implementation

Signal Edge Telecom is in full compliance with STIR/SHAKEN requirements as defined under 47 C.F.R. § 64.6301(a)(1) and (2). Our outbound calls are signed with appropriate attestation levels and routed through interconnected IP-based networks that support STIR/SHAKEN. We maintain complete operational integration of these protocols and enforce internal safeguards to prevent misuse.

II. Handling of Traceback Requests

We maintain active participation with the Industry Traceback Group (ITG) and promptly respond to all traceback requests within 24 hours. Signal Edge has a dedicated team, overseen by the Compliance Director, responsible for investigating and providing the necessary call data. We log all traceback activity and maintain full transparency with law enforcement and regulatory bodies.

III. Cooperation Clauses in Carrier Agreements

All interconnection and service agreements include clauses mandating full cooperation with traceback requests and the obligation to identify upstream providers or originating customers. These agreements ensure shared accountability and rapid escalation when illegal traffic is detected.

IV. Advanced Customer Vetting and KYC Program

Signal Edge implements a rigorous Know Your Customer (KYC) program, applicable to all retail and wholesale customers:

Business Identity Verification: Requires submission of articles of incorporation, business address, contact information, EIN, and nature of business.

Registry Verification: Wholesale clients are verified against the FCC 499-A Filer Database and the Intermediate Provider Registry. Non-listed customers are subjected to additional investigation.

Traffic Profile Review: Assessment of expected traffic patterns, volume, call destinations, and call types during onboarding.

On-Site Inspection: For high-risk entities, especially wholesale clients, we reserve the right to conduct physical inspections.

Ongoing Monitoring: Regular reassessment of customer profiles based on call behavior and compliance history.

V. Call Authentication and Origin Validation

To protect against spoofing and fraudulent usage:

Caller ID Usage Controls: Only numbers directly provisioned by Signal Edge or vetted underlying carriers are permitted for use.

Infrastructure Controls:

Single-Line Subscribers: Calls can only originate from the assigned number.

Multi-Line Systems: Outbound calls must match authorized and assigned numbers.

Call Branding Verification: Caller ID names must match the customer's registered trade or business name.

VI. Real-Time Monitoring and Analytics

Signal Edge employs a multi-layered analytics approach, combining in-house tools with third-party services to detect and block robocalls:

Traffic Analysis Metrics:

High short-duration call volumes

Low answer and completion rates

Sequential number dialing

Repetitive calls to DNC or unallocated numbers

Traffic anomalies from specific accounts

Immediate Actions:

Initiation of traceback

Blocking and blacklisting

Suspension of accounts

Reporting to law enforcement if applicable

VII. Third-Party Call Analytics Provider

Vendor: TNS Call Shield

System Features:

Blocks calls from unassigned, invalid, or DNC-listed numbers

Detects spoofing, spam-likely calls, and robocall bursts

Integrates with our network for real-time threat detection

We supplement TNS Call Shield data with internal alerting systems for holistic protection.

VIII. Proactive Call Filtering & Blocking

Our system filters and blocks illegal robocalls based on dynamic blacklists, industry intelligence, and internal heuristics. These lists are updated daily based on current threat intelligence and reports from customers, analytics vendors, and regulatory bulletins.

IX. Customer Education and Reporting

Signal Edge provides customers with:

Guidance on identifying robocalls and spoofing

Reporting channels for suspicious calls

Educational materials via our website and email

Regular updates on compliance obligations

X. Policy on International Voice Services

Signal Edge currently does not offer international voice termination services and has no immediate plans to provide such services, reducing exposure to international robocall risks.

XI. Governance, Enforcement & Policy Controls

Signal Edge maintains the following governance controls:

Acceptable Use Policies (AUPs) and Master Service Agreements (MSAs) expressly prohibit illegal robocalling.

Enforcement rights include immediate suspension or termination of violating accounts.

Customers must comply with federal and state laws, including the TCPA, TSR, and FCC regulations.

XII. Record-Keeping and Audit Trail

All call logs, traceback responses, vetting documentation, and mitigation actions are stored for a minimum of 24 months. These records are readily available upon regulatory request.

XIII. Internal Compliance & Accountability

Conclusion

Signal Edge Telecom LLC is firmly committed to preventing, detecting, and mitigating illegal robocalls. Through continuous monitoring, rigorous customer oversight, industry cooperation, and robust technological infrastructure, we ensure full compliance with FCC rules and contribute to a more trustworthy telecommunications ecosystem.

Robocall Mitigation Plan Update (Addendum)

Effective Date: March 1, 2026

This addendum supplements the Robocall Mitigation Plan dated January 1, 2025. All prior provisions remain in full force and effect. The following enhancements have been formally implemented as of March 1, 2026.

XIV. Compromised System Detection & Response Protocol

Signal Edge Telecom LLC has implemented a documented Compromised System Response Procedure designed to detect, contain, and remediate unauthorized access or misuse of network resources.

This protocol includes:

Monitoring for SIP credential abuse and anomalous authentication attempts

IP-based authentication controls and restricted access lists

Periodic credential rotation requirements for internal systems and customer accounts

Geo-location monitoring for unauthorized foreign login attempts

Immediate suspension of affected accounts upon detection of compromise

Internal forensic review and documentation of root cause

Where applicable, Signal Edge will utilize the Secure Traceback Portal "Compromised System" (CMP) designation and will document mitigation and corrective measures taken.

XV. Enhanced Traffic Anomaly Monitoring & Escalation Controls

In addition to existing monitoring described in the primary RMP, Signal Edge has formalized escalation thresholds for anomalous traffic detection.

Monitored indicators include:

Elevated short-duration call clustering

Rapid shifts in ASR (Answer-Seizure Ratio)

ALOC (Average Length of Call) degradation

High-velocity outbound dialing bursts

Repetitive calls to sequential numbering patterns

Elevated wireless termination ratios

Increased traceback frequency

If defined thresholds are triggered, Signal Edge will immediately suspend affected campaigns or accounts, initiate internal investigation, coordinate with upstream carriers where necessary, and document corrective action prior to traffic reinstatement.

XVI. Automated & AI-Assisted Dialing Governance

Signal Edge utilizes automated and AI-assisted call management systems in compliance with all applicable federal and state laws, including TCPA requirements.

Signal Edge expressly prohibits:

Spoofing of unauthorized caller identification

Artificial evasion of carrier analytics or authentication frameworks

Manipulation of attestation protocols

All automated dialing activity is subject to internal monitoring, customer compliance review, and suspension authority where violations are suspected.

XVII. High-Risk Vertical Segmentation Controls

To reduce systemic risk, Signal Edge has implemented campaign segmentation controls for higher-risk vertical categories.

These controls include:

Dedicated DID pools by campaign classification

Prohibition of cross-vertical number reuse

Independent monitoring of traffic metrics per campaign category

Enhanced review procedures for wireless-targeted campaigns

Immediate suspension protocols upon elevated complaint or traceback activity

XVIII. Formal Kill-Switch Policy

Signal Edge maintains authority to immediately suspend traffic at the campaign, account, or network level if elevated traceback frequency, upstream carrier notification indicating potential illegal traffic, significant spam-labeling spikes, or STIR/SHAKEN authentication anomalies occur. Traffic may only resume following documented review and corrective action.

Approved and Implemented as of March 1, 2026.

Certification & Approval

Approved and Implemented as of March 1, 2026.