

ROBOCALL MITIGATION PROGRAM

Regulatory Compliance & Traffic Integrity Framework

Company Address:

900 Haddon Ave
Collingswood, NJ 08018
United States

Effective Date: March 3, 2026

1. Regulatory Foundation & Legal Authority

This Robocall Mitigation Program is implemented in accordance with the rules and orders of the Federal Communications Commission (FCC), including but not limited to:

- 47 CFR § 64.6300 (Robocall Mitigation Database Requirements)
- TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence Act)
- STIR/SHAKEN Implementation Mandates
- FCC Orders 20-136, 21-122, and subsequent amendments

The company certifies its compliance with FCC requirements and affirms that it has implemented a comprehensive mitigation framework reasonably designed to prevent the origination and transmission of illegal robocalls.

2. Scope of Operations

The company operates as a VoIP telecommunications service provider facilitating voice traffic over IP-based infrastructure. The company:

- Does not knowingly originate illegal robocalls

- Does not permit customers to transmit unlawful prerecorded or artificial voice calls
 - Provides services subject to strict customer vetting and monitoring controls
-

3. STIR/SHAKEN Call Authentication Implementation

3.1 Network Authentication

The company has implemented the STIR/SHAKEN framework across its IP network infrastructure where technically feasible.

3.2 Attestation Standards

Calls are signed with appropriate attestation levels:

- **Full Attestation (A)** – When the company has verified customer identity and has established a direct relationship.
- **Partial Attestation (B)** – When customer identity is verified but call origination control is limited.
- **Gateway Attestation (C)** – When calls enter from external networks without direct authentication authority.

3.3 Certificate Governance

The company maintains active SPC tokens and authorized certificates from approved certification authorities.

4. Customer Due Diligence & Onboarding Controls

A formal Know-Your-Customer (KYC) and risk evaluation process is applied before service activation.

4.1 Required Documentation

- Legal entity registration documents

- EIN or equivalent tax identification
- Government-issued identification (where applicable)
- Business use case disclosure
- Traffic type declaration
- Beneficial ownership identification

4.2 Risk Profiling

Each applicant undergoes internal risk scoring based on:

- Industry classification
- Geographic risk factors
- Prior telecom abuse history
- Intended traffic patterns

High-risk entities are either rejected or subject to enhanced monitoring and restricted permissions.

5. Traffic Monitoring & Analytics

The company employs automated and manual monitoring systems to identify anomalous or unlawful call activity.

5.1 Real-Time Indicators

Monitoring systems track:

- Abnormal call volumes
- Short duration call bursts
- High answer-seizure ratio anomalies

- Sequential dialing behavior
- High complaint or blocking rates

5.2 Analytics & Reporting Tools

The company utilizes internal traffic analysis software and third-party analytics platforms to flag suspicious behavior.

6. Complaint Handling & Enforcement

6.1 Complaint Intake

Complaints may be received through:

- Direct consumer reports
- Carrier notifications
- Industry consortium alerts
- Government agency communications

6.2 Investigation Protocol

Upon detection of suspicious activity:

1. Immediate traffic review is conducted.
2. Customer is contacted for explanation and documentation.
3. If risk is confirmed, traffic suspension occurs immediately.

6.3 Zero-Tolerance Policy

Illegal robocalling activity results in:

- Immediate suspension

- Account termination
 - Reporting to upstream providers
 - Cooperation with law enforcement where required
-

7. Traceback Response Commitment (24-Hour Mandatory Compliance)

The company maintains a strict internal policy requiring response to all traceback requests within **24 hours without exception**.

7.1 Traceback Authorities

The company cooperates fully with:

- The FCC
- The Industry Traceback Group (ITG)
- Law enforcement agencies
- Upstream and downstream carriers

7.2 Response Procedure

Upon receipt of a traceback request:

1. Immediate acknowledgment is issued.
2. Call detail records (CDRs) are retrieved.
3. Customer attribution is identified.
4. Relevant documentation is provided to requesting authority.

Failure to respond within 24 hours is not permitted under internal compliance policy.

8. Record Retention

The company maintains:

- Call Detail Records (CDRs)
- SIP signaling logs
- IP address records
- Customer onboarding documentation

Retention period: Minimum 24 months or longer if legally required.

9. Upstream & Downstream Carrier Compliance

The company:

- Transmits traffic only through compliant upstream carriers
 - Confirms RMD (Robocall Mitigation Database) registration status of interconnected partners
 - Immediately blocks traffic from non-compliant carriers upon notification
-

10. Internal Governance & Compliance Oversight

A designated Compliance Officer oversees:

- Robocall mitigation enforcement
- FCC regulatory updates
- Customer compliance audits
- STIR/SHAKEN certificate management

Quarterly compliance reviews are conducted to ensure program effectiveness.

11. Ongoing Program Enhancements

The company commits to:

- Updating mitigation controls as FCC rules evolve
- Implementing new industry best practices
- Participating in industry-led anti-robocall initiatives
- Enhancing analytics detection models

12. Certification Statement

The company certifies that this Robocall Mitigation Program is accurate, operational, and actively enforced. The program is reasonably designed to prevent customers from using the company's network to originate illegal robocalls.

This plan is submitted in good faith to comply with FCC requirements for inclusion in the Robocall Mitigation Database.