



STELLAR
BROADBAND

**SPARTAN NET CO.
d/b/a STELLAR BROADBAND**

ROBOCALL MITIGATION PLAN
(FCC Robocall Mitigation Database Filing)

Submitted to:

Federal Communications Commission
Wireline Competition Bureau

Pursuant to:

47 C.F.R. § 64.6305
The TRACED Act

Principal Office:

3032 East Lake Lansing Road
East Lansing, Michigan 48823

Prepared as of:

March 25th, 2026

TABLE OF CONTENTS

I.	- Introduction
II.	- Scope of Application
III.	- Network Architecture
IV.	- STIR/SHAKEN Implementation
V.	- Attestation Policy
VI.	- Know Your Customer (KYC)
VII.	- Know Your Upstream Providers (KYUP)
VIII.	- Traffic Monitoring and Analytics
IX.	- Mitigation and Enforcement Procedures
X.	- Traceback Cooperation
XI.	- Recordkeeping
XII.	- CoreDial Compliance Alignment
XIII.	- Michigan Regulatory Compliance
XIV.	- Governance
XV.	- Certification
XVI.	- Authorized Officer Certification



I. INTRODUCTION

Spartan Net Co., d/b/a STELLAR Broadband (the “Company”), a Michigan corporation, hereby adopts this Robocall Mitigation Plan (the “Plan”) in accordance with applicable federal law and regulatory requirements.

This Plan is intended to demonstrate the Company’s compliance with:

- The Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (the “TRACED Act”);
- Section 64.6305 of the Federal Communications Commission (“FCC”) rules; and
- The FCC Robocall Mitigation Database (“RMD”) filing requirements.
- Michigan Consumer Protection Act (MCL 445.901 et seq.)

This Plan describes the reasonable and effective steps implemented by the Company to prevent the origination, transmission, and facilitation of illegal robocalls.

II. SCOPE OF APPLICATION

This Plan applies to all voice traffic originated, transmitted, or processed by the Company, including:

- Outbound traffic originated by customers
- Inbound traffic received from upstream providers
- Transit traffic carried across the Company’s network

III. NETWORK ARCHITECTURE

The Company operates as a VoIP service provider utilizing the CoreDial “CoreNexa” hosted platform, which is built on an Asterisk based switching architecture.

The Company’s network capabilities include:

- SIP-based call routing and switching
- Integrated STIR/SHAKEN authentication and verification



- Real-time call monitoring and analytics
- Call Detail Record (CDR) generation and retention
- Fraud detection and anomaly identification

Notwithstanding its use of third-party infrastructure, the Company retains full responsibility for:

- Customer onboarding and validation
- Traffic monitoring and mitigation
- Regulatory compliance

IV. STIR/SHAKEN IMPLEMENTATION

The Company certifies that:

- STIR/SHAKEN is implemented across all IP-originated traffic supported by its platform and upstream provider integration.
- All eligible outbound calls are signed using appropriate attestation levels; and
- Inbound calls are verified using STIR/SHAKEN Identity headers.

The Company utilizes authentication services through its platform and upstream carrier relationships.

For traffic not capable of STIR/SHAKEN authentication, the Company applies alternative mitigation measures as described herein.

V. ATTESTATION POLICY

The Company assigns STIR/SHAKEN attestation levels as follows:

A. Full Attestation (A-Level)

Applied where:

- The Company has a direct relationship with the customer; and
- The Company has verified the customer's authorization to use the calling number.
- For calls originating from the Company's network, and calls whose Caller ID is a phone number supplied by the Company, Calls are assigned Attestation level A.



B. Partial Attestation (B-Level)

Applied where:

- A direct relationship exists; but
- Number authorization cannot be fully verified.
- Sip trunks that can set passthrough/caller id/forwarded calls will be assigned Attestation Level B.

C. Gateway Attestation (C-Level)

Applied where:

- The Company acts as an intermediate provider; and
- Caller identity cannot be authenticated.

Attestation levels are continuously evaluated by our upstream provider and adjusted based on customer behavior and risk indicators.

VI. KNOW YOUR CUSTOMER (KYC)

The Company maintains a comprehensive Know Your Customer (“KYC”) program.

A. Customer Verification

- Verification of legal entity status and legitimacy
- Review of formation documents and public records
- Validation of business address
- Identification of responsible individuals

B. Risk Assessment

- Evaluation of intended use cases
- Identification of high-risk traffic profiles, including:
 - Lead generation
 - Autodialing
 - High-volume outbound calling



C. Enhanced Due Diligence

- Additional verification for high-risk customers
- Controlled service activation and staged enablement

D. Ongoing Monitoring

- Continuous monitoring of customer traffic patterns
- Identification of abnormal usage or call volumes
- Immediate review upon detection of anomalies

E. Account Controls

- Limitation of new account capabilities until verification is complete

VII. KNOW YOUR UPSTREAM PROVIDERS (KYUP)

The Company verifies upstream providers are compliant and listed in the FCC Robocall Mitigation Database.

Current Upstream Providers:

- PayG LLC d/b/a SkySwitch (RMD0002940)
- CoreDial LLC (RMD0002771)
- 123.Net, Inc. (RMD0004725)

The Company:

- Monitors inbound traffic from upstream providers
- Requires compliance through contractual obligations
- Does not knowingly accept traffic from non-compliant providers

VIII. TRAFFIC MONITORING AND ANALYTICS

The Company utilizes CoreDial platform tools and internal systems to monitor traffic in real time.



Monitored Indicators Include:

- High call volumes or burst traffic
- Short duration calls
- Repeated failed call attempts
- STIR/SHAKEN verification failures
- Geographic anomalies
- Answer-Seizure Ratio (ASR) irregularities

Threshold-Based Monitoring

Traffic is evaluated against internal thresholds for:

- Calls per second/minute
- ASR
- Average Call Duration (ACD)

IX. MITIGATION AND ENFORCEMENT PROCEDURES

The Company maintains a structured escalation process:

A. Detection

Company and CoreDial will immediately investigate any identified calls to determine if the caller is attempting to originate unlawful robocalls. If it is determined that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service appropriately.

B. Investigation

- Review of call detail records
- Analysis of traffic patterns
- Customer account review

C. Customer Notification

Customers are notified and may be required to provide:



- Number authorization documentation
- Consent records

D. Mitigation Actions

The Company may:

- Block originating or terminating numbers
- Restrict or suspend trunks
- Throttle or block traffic
- Suspend or terminate customer accounts

E. Enforcement Authority

The Company reserves the right to:

- Refuse traffic from any party
- Terminate service relationships
- Block spoofed or invalid originating numbers

X. TRACEBACK COOPERATION

The Company will fully cooperates with:

- FCC Enforcement Bureau
- Law enforcement agencies
- Industry Traceback Group (ITG)
- Private Traceback Group (TPTG)

Commitments:

- Respond to all traceback requests within twenty-four (24) hours
- Provide complete and accurate information
- Assist in identifying and mitigating illegal robocalls



STELLAR
BROADBAND

Enforcement Bureau Notifications

STELLAR Network Operations

traceback@stellarbb.com

517-203-3096

Upon notification:

- The Company will block identified illegal traffic
- The Company will block substantially similar traffic on an ongoing basis

If traffic is determined not to be illegal, the Company will provide:

- A written explanation of its determination
- Documentation of investigative steps

XI. RECORDKEEPING

The Company maintains records for reported incidents including:

- Customer onboarding documentation
- Traffic logs
- Mitigation actions
- Traceback responses

Retention Period

- Not less than twenty-four (24) months

XII. COREDIAL COMPLIANCE ALIGNMENT

The Company aligns its operations with CoreDial requirements, including:

- Strict onboarding controls
- Continuous monitoring
- Rapid mitigation procedures



- Adherence to acceptable use policies

The Company acknowledges that non-compliance may result in upstream enforcement actions, including traffic blocking.

XIII. MICHIGAN REGULATORY COMPLIANCE

The Company complies with applicable Michigan law, including:

- Michigan Consumer Protection Act (MCL 445.901 et seq.)
- Applicable telemarketing and consumer protection requirements

The Company cooperates with:

- The Michigan Attorney General
- Applicable state authorities

XIV. GOVERNANCE

- This Plan is reviewed annually or upon regulatory change
- Personnel are trained in robocall mitigation obligations
- Compliance oversight is maintained internally

XV. CERTIFICATION

The Company certifies that:

- This Plan has been implemented in good faith;
- The Company complies with 47 C.F.R. § 64.6305;
- The Company has implemented KYC, KYUP, and traffic monitoring controls;
- The Company does not knowingly originate or transmit illegal robocalls; and
- All voice traffic is subject to this mitigation program.



STELLAR
BROADBAND

XVI. AUTHORIZED OFFICER CERTIFICATION

IN WITNESS WHEREOF, the undersigned, being duly authorized, hereby certifies on behalf of Spartan Net Co., d/b/a STELLAR Broadband that the foregoing Robocall Mitigation Plan is true, accurate, and implemented in good faith.

SPARTAN NET CO., d/b/a STELLAR BROADBAND

By: *Richard Laing*

Name: Richard Laing

Title: President

Date: March 25th, 2026

Principal Business Address:

3032 East Lake Lansing Road
East Lansing, Michigan 48823