

VOXIUM TELECOM

ROBOCALL MITIGATION PLAN

2026

Prepared in accordance with Federal Communications Commission (FCC) requirements, the TRACED Act, STIR/SHAKEN caller authentication obligations, TCPA compliance standards, and telecommunications industry operational compliance expectations.

Company Information

Company Name: VOXIUM TELECOM

Responsible Officer: Rita A Gill

Business Address: 7901 4TH ST N STE 300 ST PETERSBURG, FL 33702

Business Contact Number: +1 (802) 222-6344

Employer Identification Number (EIN): 33-2497226

FCC Registration Number (FRN): 0036431351

FCC 499A Filer ID: 837395

1. Executive Summary

VOXIUM TELECOM has established and implemented this detailed Robocall Mitigation Plan as part of its commitment to protecting consumers, preserving confidence in telecommunications services, maintaining responsible network practices, supporting lawful communications activity, and complying with all applicable Federal Communications Commission (FCC) regulations relating to illegal robocalling, caller ID spoofing, telecommunications fraud, phishing-related traffic, and unlawful automated calling activity. This document outlines the company's operational compliance procedures, STIR/SHAKEN caller authentication controls, customer verification standards, traceback cooperation commitments, fraud prevention methodologies, traffic monitoring procedures, DNO protections, TCPA compliance controls, and telecommunications security practices intended to reduce unlawful telecommunications traffic and support ongoing regulatory compliance obligations. VOXIUM TELECOM continuously reviews and updates its operational compliance framework to align with evolving FCC guidance, telecommunications security concerns, industry best

practices, and robocall mitigation expectations.

2. Regulatory Compliance Commitment

VOXIUM TELECOM is committed to maintaining compliance with all applicable federal telecommunications laws, regulations, and operational guidance relating to robocall mitigation, caller authentication, telecommunications fraud prevention, and consumer protection obligations. The company supports and complies with requirements established by: • The Federal Communications Commission (FCC) • The Telephone Consumer Protection Act (TCPA) • The TRACED Act • STIR/SHAKEN caller authentication obligations • Industry traceback cooperation standards • Telecommunications fraud prevention frameworks • Applicable telecommunications compliance standards The company continuously monitors evolving telecommunications regulations and compliance expectations to ensure that internal operational procedures remain aligned with industry best practices and regulatory requirements.

3. Operational Structure and Provider Classification

VOXIUM TELECOM operates as a Hybrid Telecommunications Provider and may function in multiple operational roles within the telecommunications ecosystem depending upon customer relationships, traffic origination methods, network routing structures, and interconnected carrier arrangements. The company may operate as: • A Wholesale Voice Provider • An Intermediate Telecommunications Provider • A Retail Telecommunications Service Provider • A VoIP Service Provider • A Gateway Provider • An Interconnected Carrier VOXIUM TELECOM may originate, terminate, exchange, route, transport, or transmit domestic and international telecommunications traffic through interconnected telecommunications infrastructure and VoIP-based systems. Operational services provided by the company may include: • SIP trunking services • Domestic voice routing • International telecommunications services • DID-related telecommunications services • Carrier interconnection support • Telecommunications exchange and routing services The company does not knowingly facilitate unlawful robocalling activity, illegal caller ID spoofing, phishing campaigns, scam-related telecommunications traffic, or fraudulent telecommunications communications.

4. Customer Due Diligence and KYC Procedures

VOXIUM TELECOM maintains a comprehensive Know Your Customer (KYC) and customer verification framework intended to reduce telecommunications fraud risk, network misuse, unlawful robocalling activity,

caller ID spoofing, and suspicious telecommunications behavior. Prior to activating telecommunications services, the company may conduct customer verification and onboarding procedures including:

- Verification of legal business registration
- Validation of EIN and FCC registration information
- Review of operational legitimacy
- Verification of business contact information and addresses
- Website and domain verification procedures
- Payment verification measures
- Review of telecommunications use cases
- Compliance screening and fraud review
- Review of traceback or enforcement history where applicable

Operational legitimacy review procedures The company reserves the right to suspend, deny, restrict, or terminate telecommunications services associated with suspicious, unlawful, misleading, fraudulent, or non-compliant activity. Equivalent compliance expectations may also be applied to interconnected providers, upstream carriers, telecommunications vendors, and operational partners.

5. STIR/SHAKEN Caller Authentication and Attestation Framework

VOXIUM TELECOM maintains a fully STIR/SHAKEN-enabled telecommunications infrastructure in compliance with applicable FCC caller authentication obligations and telecommunications industry standards. The company applies caller attestation standards based upon customer authentication controls, operational verification procedures, and telecommunications traffic review processes. Full Attestation (A-Level): “A” attestation is applied where VOXIUM TELECOM maintains a direct authenticated relationship with the originating customer, has verified the customer identity, and has validated the customer’s authorization to utilize the calling number presented. Partial Attestation (B-Level): “B” attestation is applied where the company maintains a known customer relationship but cannot independently validate authorization rights relating to the calling number presented. Gateway Attestation (C-Level): “C” attestation is applied where traffic is received from interconnected providers or gateway sources and the originating end-user identity cannot be independently authenticated. VOXIUM TELECOM:

- Authenticates caller identity information where applicable
- Preserves STIR/SHAKEN identity headers throughout the call path
- Reviews suspicious or improperly authenticated traffic
- Monitors unsigned traffic for fraud indicators
- Maintains caller authentication integrity procedures
- Reviews irregular telecommunications signaling behavior
- Supports industry-wide caller authentication standards

Unsigned, suspicious, spoofed, or irregular telecommunications traffic determined to present elevated fraud risk may be blocked, restricted, suspended, or subjected to additional compliance review procedures where operationally appropriate.

6. Telecommunications Traffic Monitoring and Network Analytics

VOXIUM TELECOM maintains proactive traffic monitoring systems and analytics-based operational review procedures intended to identify suspicious telecommunications behavior and unlawful robocalling activity. Traffic monitoring procedures may include analysis of:

- High-volume call pattern monitoring
- Sequential dialing analysis
- Short-duration call detection
- Geographic anomaly review
- Routing irregularity monitoring
- Suspicious ANI presentation review
- Fraud-related signaling analysis
- Telecommunications abuse detection
- Repetitive call behavior monitoring
- Unusual traffic routing patterns
- Elevated fraud-risk telecommunications behavior

Traffic identified as potentially harmful, suspicious, abusive, fraudulent, or non-compliant may be investigated, restricted, blocked, suspended, or terminated where operationally appropriate. The company continuously reviews operational traffic activity to identify potential compliance concerns and fraudulent telecommunications patterns.

7. Fraud Prevention and DNO Protection Measures

VOXIUM TELECOM maintains fraud prevention procedures and continuously updated Do-Not-Originate (DNO) protections intended to reduce unlawful caller ID spoofing, telecommunications abuse, and fraudulent telecommunications activity. The company maintains procedures intended to identify and block:

- Invalid telephone numbers
- Unallocated or unassigned numbers
- Inbound-only numbers
- Unauthorized outbound caller IDs
- Emergency service-related spoofing attempts
- Fraud-associated telecommunications traffic
- Invalid caller identification information
- Potentially spoofed traffic activity
- Suspicious signaling behavior
- Fraud-related telecommunications routing patterns

DNO protections and fraud mitigation controls are periodically reviewed and updated as part of the company's broader telecommunications fraud prevention and robocall mitigation framework.

8. Traceback Cooperation and Regulatory Response Procedures

VOXIUM TELECOM cooperates fully with traceback investigations and lawful telecommunications compliance inquiries relating to suspicious robocalling activity, spoofed traffic, telecommunications fraud, scam campaigns, and unlawful automated calling behavior. The company commits to responding to traceback requests from authorized regulatory agencies, the Industry Traceback Group (ITG), law enforcement agencies, and telecommunications compliance organizations within twenty-four (24) hours of receipt. Operational review procedures may include:

- Traffic investigation procedures
- Customer usage review
- Signaling analysis
- Fraud escalation procedures
- Compliance review procedures
- Restriction or suspension of suspicious telecommunications traffic
- Investigation of routing activity
- Preservation of operational compliance records

The company maintains procedures designed to ensure timely review and

response to traceback inquiries and telecommunications compliance investigations.

9. TCPA, Consent Verification, and DNC Compliance Controls

VOXIUM TELECOM expects all customers, interconnected providers, and telecommunications partners to comply with National Do-Not-Call (DNC) requirements, the Telephone Consumer Protection Act (TCPA), and applicable FCC telemarketing regulations. Where the company provides retail or end-user telecommunications services, VOXIUM TELECOM maintains reasonable compliance controls intended to support lawful communications practices and TCPA obligations. These compliance measures may include: • Customer consent verification procedures • Internal DNC compliance review measures • Pre-authorized opt-in requirements where applicable • Automated calling activity monitoring • Customer telecommunications use-case review • Telecommunications abuse complaint investigations • Restriction or suspension of unlawful telecommunications campaigns • Customer compliance oversight procedures Customers utilizing telecommunications services are expected to maintain appropriate consumer consent records and comply with all applicable federal and state telecommunications regulations.

10. Compliance Administration and Operational Oversight

VOXIUM TELECOM maintains operational compliance procedures relating to: • Customer onboarding and verification • Telecommunications traffic analytics • Traceback investigations • Fraud prevention activities • Customer traffic investigations • Telecommunications security monitoring • Compliance enforcement procedures • Operational telecommunications review measures • Telecommunications compliance oversight • Caller authentication review procedures The company periodically reviews and updates its telecommunications compliance framework to align with evolving FCC requirements, STIR/SHAKEN obligations, telecommunications industry standards, telecommunications security concerns, and robocall mitigation expectations.

11. Final Compliance Statement

VOXIUM TELECOM remains committed to supporting lawful telecommunications operations, protecting consumers, maintaining responsible network practices, and implementing effective robocall mitigation procedures designed to reduce unlawful telecommunications activity. The company will continue maintaining caller authentication integrity, fraud mitigation controls, traceback cooperation procedures,

customer verification standards, traffic monitoring systems, and operational compliance measures intended to support telecommunications security and FCC compliance obligations. VOXIUM TELECOM remains committed to maintaining compliance with applicable FCC robocall mitigation requirements, caller authentication obligations, telecommunications fraud prevention standards, and industry compliance expectations.