



Puma Telecommunications Robocall Mitigation Program

Platform Compliance Implementation

Overview

The Puma Telecommunications platform (Running on SkySwitch), maintains FCC compliance through integrated STIR/SHAKEN authentication, Nomorobo robocall blocking, comprehensive call analytics, and automated compliance reporting. This document describes the specific compliance mechanisms implemented on the Puma Telecommunications platform.

STIR/SHAKEN Authentication

Platform Implementation

Puma Telecommunications implements STIR/SHAKEN caller ID authentication on all IP network portions:

- Digital signing of outbound calls using certified authentication tokens
- Verification of inbound call authentication headers
- Preservation of authentication information through intermediate routing
- Attestation level assignment based on call origin verification

Attestation Levels

Level	Attestation	Puma Telecommunications Assignment
A	Full	Calls from verified Puma Telecommunications-provisioned DID's with authenticated customer relationships
B	Partial	Calls originating from platform but with limited caller authorization verification
C	Gateway	Calls entering platform from external sources or unverified origins

Caller ID Spoofing Policy

Puma Telecommunications blocks caller ID spoofing on the platform. Outbound calls can only display caller IDs for DID's directly provisioned and associated with the Puma Telecommunications platform. Any attempt to spoof numbers not owned by or assigned to the reseller's account is automatically blocked.

Nomorobo Robocall Blocking

Real-Time Call Screening

Puma Telecommunications integrates with Nomorobo's database to identify and block robocalls before they reach end users:

- Pre-ring identification: Caller numbers checked against Nomorobo database before phones ring
- User notification: System alerts users when incoming calls are flagged as potential robocalls
- Configurable handling: Calls can be automatically answered and dropped, sent to voicemail, or rejected
- Database updates: Continuous synchronization with Nomorobo's threat intelligence database

Reseller Configuration

Resellers can configure Nomorobo settings through the Puma Telecommunications portal:

- Enable/disable per customer or globally
- Set call handling preferences (block, voicemail, notification only)
- Whitelist specific numbers to bypass screening
- Access blocking reports and statistics

Call Analytics and Monitoring

Traffic Analysis

Puma Telecommunications monitors call traffic for suspicious patterns indicating robocall activity:

- High-volume calling pattern detection
- Sequential dialing identification
- Short-duration call monitoring
- Geographic anomaly detection
- Automated alerting for abnormal traffic

Enforcement Actions

When suspicious activity is detected, Puma Telecommunications implements automated mitigation:

- Rate limiting on accounts showing robocall patterns
- Automatic notification to reseller account administrators
- Temporary service suspension for severe violations
- Documentation of incidents for regulatory reporting

Robocall Mitigation Database Compliance

Puma Telecommunications RMD Filing

Puma Telecommunications maintains its own certification in the FCC's Robocall Mitigation Database:

- Current certification documenting STIR/SHAKEN implementation status
- Detailed robocall mitigation plan filed and maintained
- CORES registration kept current with 10-business-day update requirement
- Automated monitoring to ensure certification remains active

Reseller Support

Puma Telecommunications provides resellers with resources for their independent RMD compliance:

- Documentation of platform STIR/SHAKEN implementation for reseller RMD submissions
- Technical specifications for robocall mitigation plan development
- Guidance on reseller certification requirements
- Support team assistance with compliance questions

Traceback and Investigation Support

Traceback Response System

Puma Telecommunications maintains systems to respond to industry traceback requests:

- Call detail record retention for regulatory compliance periods
- Dedicated traceback response team and procedures
- Integration with industry traceback consortiums
- Automated call origination tracking through the platform

Reseller Coordination

When traceback requests involve reseller customers:

- Puma Telecommunications identifies the responsible reseller account
- Automated notification sent to reseller administrators
- Call detail records provided for reseller investigation
- Coordination with reseller on response to traceback consortiums

Customer Vetting and Account Security

Reseller Account Controls

Puma Telecommunications provides resellers with tools to vet and manage their customers:

- Account creation review and approval workflows
- Service usage monitoring and reporting per customer
- Configurable rate limits and calling restrictions
- Emergency suspension capabilities for problematic accounts
- Customer agreement template provisions for acceptable use

DID Provisioning Controls

All DIDs provisioned through Puma Telecommunications are subject to ownership verification and assignment controls. The platform maintains association records between DIDs and reseller accounts, preventing unauthorized number usage and supporting STIR/SHAKEN attestation accuracy.

Network Security and Access Controls

Platform Security Measures

Puma Telecommunications implements security controls to prevent unauthorized platform access:

- Multi-factor authentication for administrative access
- IP whitelisting and geographic access restrictions
- Encrypted SIP signaling (TLS) and media streams (SRTP)
- Regular security audits and vulnerability assessments
- Intrusion detection and prevention systems

Upstream Carrier Verification

Puma Telecommunications verifies that all upstream carriers and interconnection partners maintain active RMD certifications. Traffic is only accepted from providers listed in the FCC Robocall Mitigation Database, ensuring compliance throughout the call chain.

Documentation and Reporting

Compliance Documentation

Puma Telecommunications maintains comprehensive documentation of compliance measures:

- Platform STIR/SHAKEN implementation specifications
- Robocall mitigation procedures and protocols
- Incident response and enforcement action logs
- Traceback response records and timelines
- Regulatory filing history and updates

Reseller Reporting Tools

Resellers have access to reports supporting their compliance obligations:

- Call traffic analytics and volume reports
- Nomorobo blocking statistics and trends
- STIR/SHAKEN attestation level distribution
- Customer usage patterns and anomaly alerts
- Export capabilities for regulatory submissions

Ongoing Compliance Maintenance

Platform Updates

Puma Telecommunications continuously updates compliance mechanisms to meet evolving regulations:

- Regular review of FCC orders and rulemaking proceedings
- Implementation of new requirements within mandated timeframes
- Testing and validation of compliance features
- RMD certification updates within 10 business days of platform changes
- Reseller notification of compliance-impacting platform updates

Industry Collaboration

Puma Telecommunications participates in industry working groups and traceback consortiums to coordinate robocall mitigation efforts across the telecommunications ecosystem. This includes sharing threat intelligence, best practices, and coordinating responses to emerging robocall campaigns.

Reseller Support Resources

Technical Documentation

Available at docs.Puma Telecommunications.com:

- STIR/SHAKEN implementation guide
- Robocall Mitigation Database filing requirements
- Nomorobo configuration instructions
- Compliance FAQs and troubleshooting guides

Support Contact Information

- Technical Support: (747) 777-8102
- Sales and Account Management: (646) 663-7600
- Documentation Portal: docs.skyswitch.com

Summary

Puma Telecommunications maintains FCC compliance through integrated STIR/SHAKEN authentication (Included with the Skyswitch Platform), Nomorobo robocall blocking, comprehensive call analytics, automated threat detection, and rigorous customer vetting controls. The platform handles upstream compliance requirements while providing resellers with the tools and documentation needed to meet their independent regulatory obligations.