



CASCABEL NETWORKS LLC

Robocall Mitigation Plan

FRN: 0016323495

RMD: RMD0004188

Effective Date: 2026

Background and Regulatory Status

Cascabel Networks LLC is an international wholesale telecommunications provider serving U.S. and foreign carriers. The Company operates primarily as an intermediate provider and does not originate end-user consumer traffic. The Company does not knowingly originate or knowingly facilitate illegal robocall traffic.

The Company takes reasonable and effective steps to prevent the origination, transmission, and processing of illegal robocalls affecting traffic routed to or from the United States telecommunications network in compliance with:

1. 47 CFR § 64.6305
2. The TRACED Act
3. FCC Report and Order 20-136
4. Subsequent FCC Orders governing the Robocall Mitigation Database

A designated compliance attorney oversees implementation and reports directly to executive leadership.

This plan is designed to demonstrate reasonable mitigation efforts.

STIR/SHAKEN Implementation

As applicable under 47 CFR § 64.6304, the Company has implemented STIR/SHAKEN authentication and validation for SIP-based traffic traversing its IP network. The Company monitors attestation integrity and may block traffic with improper or invalid attestation where required.

The Company:

- Validates incoming attestation levels (A, B, and C)
- Monitors traffic patterns associated with downgraded or anomalous attestations
- Investigates repeated or improper use of full (A-level) attestation
- Blocks or restricts traffic where attestation appears fraudulent, improper, or absent without justification

JMS MHA FL AS SMA



Improper or misleading attestation is treated as a material compliance violation and may result in immediate suspension of the originating provider.

Robocall Risk Management Framework

The Company applies a risk-based mitigation approach including:

- Customer onboarding risk scoring
- Traffic pattern profiling
- Continuous anomaly detection
- Escalation thresholds

Risk Classification

Risk Level	Description
Low	Established wholesale carriers with clean compliance history and stable traffic patterns.
Medium	Providers with moderate traffic variability or higher call volume campaigns requiring closer supervision.
High	Providers or traffic patterns presenting elevated risk indicators associated with potential robocall activity.
Prohibited	Traffic or customers confirmed or reasonably suspected of illegal robocall activity or regulatory non-compliance.

High-risk classifications include:

- Auto-dialer service providers
- Political campaign traffic
- Short-duration call campaigns
- International gateway arbitrage traffic

Know Your Customer (KYC)

Pre-Activation Controls

No customer traffic is activated until completion of:

- Executed Master Services Agreement including KYC disclosures
- FCC Enforcement database review
- Robocall Mitigation Database registration verification
- Business model and call flow disclosure
- Traffic volume and dialing methodology review

Ongoing Monitoring

- Monthly risk reassessment
- Short-duration ratio monitoring

JDS MHA FC AS SMA



- ASR anomaly detection
- Complaint monitoring

Customer agreements prohibit illegal robocalls and require mandatory traceback cooperation. Failure to cooperate constitutes material breach.

Know Your Upstream Provider (KYUP)

Prior to interconnection:

- Verification of Robocall Mitigation Database registration and good standing
- STIR/SHAKEN certification validation
- FCC enforcement history review
- Confirmation of traceback participation

The Company only accepts traffic from providers that are actively registered and in good standing in the Robocall Mitigation Database and requires all providers to maintain robocall mitigation practices consistent with FCC regulations. Non-compliant upstream providers may have their traffic blocked or interconnections suspended, and all partners must fully cooperate in traceback and mitigation investigations.

Traffic Monitoring & Analytics

The Company maintains real-time automated monitoring systems including:

- CPS thresholds
- Short-duration ratio controls
- Burst traffic detection
- Invalid/unallocated number detection
- Spoofing detection
- ASR anomaly alerts

External sources include:

- Industry Traceback Group (ITG) notifications
- FCC Enforcement Bureau advisories
- Carrier complaint exchanges

Immediate Mitigation & Escalation

Upon detection of suspicious traffic:

- Compliance review initiated within 2 hours
- Customer notification
- Traffic rate-limiting or blocking

JMS MHA FL AS SMA



If illegal traffic is confirmed:

- Immediate suspension
- Reporting to regulators when required

Traceback Commitment

The Company commits to:

- Respond within 24 hours to authorized traceback requests
- Provide complete CDRs and SIP headers where applicable
- Identify immediate upstream source
- Preserve investigative evidence
- Cooperate fully with ITG, FCC, and law enforcement

The Company maintains designated compliance and network operations personnel responsible for coordinating traceback responses. Roles and responsibilities are documented internally, and escalation procedures ensure timely resolution of suspicious traffic or enforcement requests.

Record Retention

Records are retained for a minimum of two (2) years and may be retained up to five (5) years for regulatory defense and investigation support.

Internal Controls, Audit, and Documentation

The Company maintains formal internal compliance controls including:

- Customer due diligence files
- Call Detail Record (CDR) archives
- Traceback logs and investigation records
- Regulatory reporting documentation
- Executive compliance review summaries

An internal compliance review is conducted on a periodic basis, including traffic analysis and mitigation effectiveness assessment.

Compliance Training Program

The Company maintains an internal robocall compliance training program that includes:

- Mandatory compliance training for relevant personnel
- Specialized training for NOC and compliance staff
- Periodic updates reflecting regulatory changes
- Executive-level compliance briefings

JMS MHA FC AS SMA



Corporate Structure Disclosure

Pursuant to applicable FCC Public Notices:

Principals:

Name	Title	Country of Residence
Simon Masri	Member	Mexico
Salomon Masri	Member	Mexico
Ernesto Polin	Member	Mexico
Ricardo Flores	Member	United States

Affiliates: None

Subsidiaries: None

Parent Company: None

Program Review and Updates

This Plan is reviewed:

- Annually
- Following FCC rule changes
- Following enforcement inquiries

The Company will update its RMD certification within 10 business days of any material change.

Executive Certification

I certify under penalty of perjury that the Company has implemented the mitigation practices described herein and that the information provided is true and accurate.

A handwritten signature in black ink, appearing to read 'AS', is positioned above a horizontal line.

Abraham Smeke
CEO C3ntro Global

JSJS JAH FL SML