



ROBOCALL MITIGATION PLAN

1. Filer Information

Legal Company Name: RAVN Enterprises Inc., d/b/a Milo Communications

FCC Registration Number (FRN): 0038106589

FCC Form 499 Filer ID: 838717

Operating Company Number (OCN): Pending

Headquarters Address: 14001 W State Hwy 29 #102, Liberty Hill, TX 78642, USA

Provider Category: Non-facilities-based interconnected VoIP reseller

Designated Compliance Contact: Rojeen Manzoori - COO

Compliance Contact Phone / Email: 403-466-4920 / rojeen@milocommunications.com

Underlying Network/Platform Partner(s): One or more third-party wholesale VoIP/interconnection providers (identity retained in the Company's internal compliance records)

2. Certification Statement

RAVN Enterprises Inc., d/b/a Milo Communications ("the Company"), hereby certifies the following in connection with its filing in the FCC's Robocall Mitigation Database:

- All voice calls that the Company originates on the public switched telephone network (PSTN) are subject to a robocall mitigation program that meets the requirements of 47 C.F.R. § 64.6305.
- The Company has not had any prior Robocall Mitigation Database certification removed or invalidated by Commission action.
- The Company has not been prohibited, in whole or in part, from filing in the Robocall Mitigation Database by the Commission or any court.
- The information provided in this Plan and in the associated Robocall Mitigation Database filing is true, accurate, and complete to the best of the Company's knowledge, and the Company understands its obligation to update this filing within 10 business days of any material change.

3. STIR/SHAKEN Implementation Status

The Company is a non-facilities-based reseller of interconnected VoIP service. It does not own or operate the underlying IP network, softswitch, or session border controllers used to originate, route, or terminate customer calls; these are owned and operated by one or more third-party underlying carrier/platform partners engaged by the Company from time to time.

Implementation status on the IP portions of the network used to provide service:

- Partial Implementation — The Company's underlying carrier partner(s) have implemented STIR/SHAKEN call authentication on the IP network segments they control. The Company itself does not directly control SIP signaling infrastructure and therefore relies on its underlying carrier partner(s)' attestation practices for the portions of the call path it does not own.

Because the Company cannot independently attest calls at the network layer, it satisfies its obligation through the robocall mitigation program described in Section 4 below, consistent with 47 C.F.R. § 64.6305(b), which permits non-facilities-based providers unable to implement STIR/SHAKEN directly to rely on a documented mitigation program.

4. Robocall Mitigation Program — Reasonable Steps

The Company has implemented the following reasonable steps to avoid originating, carrying, or processing illegal robocall traffic:

4.1 Know Your Customer (KYC) Onboarding

- Verification of business identity, physical address, and authorized contact for every customer prior to activating outbound calling service.
- Collection and retention of signed service agreements identifying the customer's intended use case and expected calling patterns (e.g., hospitality front desk, senior living facility line, corporate office).
- Refusal to provision service to prospective customers who cannot provide verifiable business identity or who request configurations consistent with mass unsolicited outbound calling.
- Re-verification of customer identity and use case upon any material change in account ownership or calling behavior.

4.2 Call Pattern Monitoring and Anomaly Detection

- Ongoing monitoring of customer call volumes, call duration patterns, and destination dispersion for deviations from the expected profile established at onboarding.
- Automated or manual flagging of accounts exhibiting sudden volume spikes, abnormally short call durations, high failed-call ratios, or sequential/random dialing patterns indicative of robocalling.
- Suspension of outbound calling capability for accounts pending investigation when anomalous patterns are detected, with restoration only after the customer's use case is confirmed legitimate.

4.3 Traceback Cooperation

- Designation of the compliance contact identified in Section 1 as the Company's single point of contact for traceback requests from the Industry Traceback Group (USTelecom), the FCC, or state/federal law enforcement.
- Commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, including identification of the immediate upstream source or customer associated with flagged traffic.
- Retention of call detail records sufficient to support traceback requests for the period required under applicable Commission rules.

4.4 Contractual Safeguards with Underlying Carrier/Platform

- Service agreements with the Company's underlying carrier/platform partner(s) require each such partner to notify the Company of any traceback requests, traffic-blocking actions, or suspected illegal traffic associated with the Company's numbering resources.
- The Company reserves the right to immediately suspend service to any customer identified as a source of illegal robocall traffic, consistent with its terms of service.

4.5 Employee Training and Internal Escalation

- Personnel responsible for customer onboarding and account management are trained to recognize indicators of potential robocalling or spoofing misuse and to escalate suspected violations to the designated compliance contact.
- The Company maintains an internal escalation path for handling consumer complaints regarding suspicious or unwanted calls traced to its numbering resources.

5. Consumer Complaint Handling

The Company investigates consumer or downstream-provider complaints regarding calls traced to its service within a reasonable time of receipt, and will suspend or terminate service to any customer confirmed to be the source of illegal robocall traffic.

6. Annual Recertification and Updates

The Company will recertify this filing on an annual basis by the deadline established by the Commission (currently March 1) and will update this Plan and the associated Robocall Mitigation Database entry within 10 business days of any material change in the information provided herein, including changes in underlying carrier/platform, STIR/SHAKEN implementation status, OCN assignment, or compliance contact.

7. Signature



Name: Rojeen Manzoori

Title: COO

Company: RAVN Enterprises Inc., d/b/a Milo Communications

Date: July 28, 2026