

Robocall Mitigation Plan for Cloud One PBX LLC
Updated as of September 01, 2026

Introduction

Cloud One PBX LLC ("COPL"), a small cloud-based Unified Communications as a Service (UCaaS) provider, offers retail hosted PBX services exclusively to end-user business customers in the United States. COPL does not provide SIP trunking, wholesale services, origination for resellers, or act as an intermediate provider in any call path. COPL does not accept any foreign-originated traffic and operates solely with domestic U.S. NANP resources for retail end-users. As a small provider without its own Class 4 switch or least-cost routing platform, COPL relies on trusted underlying carriers (e.g., SIP.US AKA BCM ONE) for DID origination, call termination, and STIR/SHAKEN attestation/signing.

This Robocall Mitigation Plan outlines COPL's measures to detect, prevent, and mitigate unlawful robocalls in compliance with FCC regulations, including section 64.6305 and the updated requirements from the 2025 Robocall Mitigation Database Report and Order (effective February 5, 2026, with first annual recertification due March 1, 2026). COPL's retail-only model and end-user focus result in inherently low robocall risk, as customers use services for standard business communications rather than high-volume outbound campaigns.

1. Contact Information

Cloud One PBX LLC
Address: 5 Brewster St, Unit 2 Number 257, Glen Cove NY 11542
Primary Contact Name: Ralph DiCaterino
Email Address: [ralphd @ tel- one.com](mailto:ralphd@tel-one.com)
Phone: 516-801-3030

Principals, Affiliates, Subsidiaries, and Parent Companies:

John DiCaterino
Ralph DiCaterino
Tel-One Communications Inc

COPL affirms that neither it nor any affiliated entity has been subject to FCC or law enforcement action related to illegal robocalling, spoofing, or RMD deficiencies in the past two years.

- 2. Implementation of STIR/SHAKEN Framework** COPL complies with FCC STIR/SHAKEN caller authentication requirements through its underlying carrier

partnerships (e.g., SIP.US AKA BCM ONE). As a small retail UCaaS provider without direct control over origination signing infrastructure:

- All outbound calls from COPL's hosted PBX environment are authenticated and signed by the underlying carrier using appropriate attestation levels (typically A for verified customer DIDs).
 - COPL's customers benefit from enhanced call trust and integrity via this upstream implementation.
 - COPL certifies partial STIR/SHAKEN implementation (Option 2 in RMD) for IP portions of the network, relying on upstream providers for technical attestation/signing. COPL makes all attestation-level decisions based on verified customer right-to-use of DIDs and provides this information to the upstream carrier for signing using COPL's upstream relationship. COPL does not maintain its own SPC token or certificate, as this is unnecessary and disproportionate for a small retail provider without wholesale or high-volume origination and no facilities-based IP origination infrastructure.
 - COPL confirms no previous certification has been removed by Commission action.
3. **Robocall Monitoring and Mitigation** COPL prevents illegal robocalls through basic monitoring and customer controls appropriate to its small retail UCaaS model:

Traffic Monitoring

- Relies on underlying carriers' real-time analytics (SIP.US AKA BCM ONE platform) to flag anomalies (e.g., high volumes, short durations, suspicious patterns, ASR/ACD deviations, call velocity, snowshoeing). COPL receives and reviews all high-risk alerts within 4 hours and takes immediate action. Independent advanced analytics are unnecessary, as retail end-user traffic is low-volume and predictable (standard business calls).

Customer Vetting

- Verifies new retail business customers' identity and intended legitimate use (e.g., business communications).
- Requires agreement to terms prohibiting illegal robocalling/TCPA violations.
- Requires all customers to agree to prohibitions on robocalling and immediately blocks any numbers identified on the FCC Do-Not-Originate (DNO) list via upstream enforcement.

- Takes steps to prevent origination of illegal calls, though retail PBX customers pose minimal risk compared to wholesale scenarios.

Complaint Resolution

- Provides a process for reporting suspected robocalls (via support channels or email).
- Investigates and takes corrective action, up to service termination if violations confirmed.

4. Call Analytics and Upstream Provider Procedures

- **Call Analytics:** COPL utilizes SIP.US AKA BCM ONE's real-time call analytics platform, which monitors ASR, ACD, call velocity, short-duration patterns, and snowshoeing. COPL receives and reviews all high-risk alerts within 4 hours and takes immediate action. As a small provider without its own switching platform, independent analytics are unnecessary and disproportionate to risk.
- **Upstream Provider Procedures:** Prior to contracting and annually thereafter, COPL verifies each upstream provider's active RMD filing, STIR/SHAKEN status, and robocall mitigation plan via the RMD portal before routing any traffic. Periodic reviews confirm ongoing compliance.

5. Compliance with FCC Requirements COPL fully complies with FCC robocall mitigation rules:

- Maintains an active filing in the FCC's Robocall Mitigation Database (RMD), including role (voice service provider serving end-users), STIR/SHAKEN status, and mitigation plan.
- **Annual Recertification:** Will recertify RMD filing annually by March 1 (first deadline March 1, 2026; window opens February 1, 2026). Recertification involves logging into the RMD portal with multi-factor authentication (required effective February 5, 2026), verifying accuracy of all information (mitigation practices, STIR/SHAKEN certification, contacts), updating if needed, and submitting via the "Recertify" button.
- **Prompt Updates:** Updates RMD and CORES registration within 10 business days of any material change (e.g., ownership, contacts), per 47 CFR § 64.6305.
- Responds fully to ITG traceback requests within 24 hours.
- Pays any required filing fees when effective

- Responds promptly to FCC deficiency notices, curing issues within specified timeframes to avoid RMD removal or traffic blocking. Noncompliance risks include base forfeitures (\$10,000 for false/inaccurate info; \$1,000 per day until cured for late updates).

6. **Future Enhancements** COPL commits to ongoing improvement:

- Monitoring upstream carrier enhancements for better analytics/blocking.
- Educating customers on robocall awareness/reporting.
- Adapting to emerging threats (e.g., AI voice cloning) via upstream partnerships and FCC guidance.

7. **Commitment to Correct Deficiencies** COPL will address any FCC-notified RMD deficiencies immediately, updating certifications/plans, explaining actions, and ensuring compliance to maintain filing status.

Conclusion Cloud One PBX LLC is dedicated to protecting its retail business customers and the public from illegal robocalls. Through reliable upstream partnerships, customer-focused controls, and full adherence to updated FCC requirements (including 2026 annual recertification by March 1), COPL provides secure, compliant hosted PBX services. As a small retail UCaaS provider with no wholesale or international elements, COPL's plan is proportionate, effective, and aligned with FCC expectations for low-risk entities.

Authorized By: Cloud One PBX LLC Compliance Team

Contact: Ralph DiCaterino, Regulatory Contact

Program Review Cycle: Annual or as required by FCC changes