



CloudNett Robocall Mitigation Program (RMP)

Updated February 24, 2026

CloudNett is a managed service provider (“MSP”) that offers limited, incidental voice services to small to mid-sized end-user customers. CloudNett originates voice traffic to the public switched telephone network (“PSTN”) and maintains a robocall mitigation program consistent with 47 C.F.R. § 64.6305. CloudNett also maintains STIR/SHAKEN caller ID authentication controls consistent with 47 C.F.R. § 64.6301(a), as further described below.

This Robocall Mitigation Plan applies to all outbound voice traffic that originates on CloudNett’s network and is limited to traffic associated with its end-user customers. CloudNett does not offer voice services on a wholesale basis and does not support reseller traffic.

STIR/SHAKEN Implementation

CloudNett certifies that it has implemented Complete STIR/SHAKEN caller ID authentication for calls it originates, consistent with 47 C.F.R. § 64.6301(a). CloudNett’s voice network is entirely IP-based, and it signs all originating calls using its STIR/SHAKEN signing certificate.

CloudNett uses third-party providers to support its STIR/SHAKEN implementation. Telonium serves as the Certificate Authority and issued the CloudNett’s signing certificate, and Telonium also performs the technological act of signing with CloudNett’s certificate.

CloudNett assigns attestation levels based on its verification of the customer relationship and the calling party’s authority to use the associated telephone number(s), consistent with applicable FCC rules and guidance.

Know Your Customer

CloudNett primarily serves established small to mid-sized business end-users and has a direct working relationship with its customers through on-site installations and ongoing managed services. Customer validation is therefore relationship-driven and supported by standard account documentation.

At onboarding and throughout the relationship, CloudNett:

- Confirms the customer’s identity and business presence through direct contact via on-site work and service management.
- Collects standard account information (legal business name/DBA, service address, responsible contact, and billing/payment details).
- Confirms the intended voice use case and expected calling behavior consistent with the customer’s business operations.
- Serves only end-users and does not support reseller or wholesale arrangements.

If call patterns, upstream notifications, traceback inquiries, or complaints indicate potential misuse, CloudNett escalates review, requests clarification and supporting documentation as needed, and may restrict, suspend, or terminate service under its acceptable use/contract terms.



Traffic Monitoring and Analytics

CloudNett uses 3CX security features, including auto-blacklisting, and standard account controls to help detect and limit suspicious calling activity. Customer accounts are provisioned and managed by CloudNett and maintained using baseline security practices, e.g., access controls, secure credentials, and routine configuration management.

Monitoring is supported by CloudNett's direct customer relationships, which enable quick validation of calling behavior against the customer's stated business use. CloudNett also relies on upstream carrier notifications as an additional indicator of suspect traffic.

If suspicious activity is identified, CloudNett investigates and may require remediation, block the affected traffic or caller IDs, suspend service, or terminate service for repeat or confirmed abuse, consistent with its acceptable use/contract terms.

Know Your Upstream Provider

CloudNett does not accept third-party traffic for transit. Outbound calls originate only from CloudNett's end users; inbound calls are received from carrier partner(s) only for delivery to those end users. CloudNett coordinates with its upstream carrier partner(s) on suspected illegal traffic and traceback requests.

Traceback Commitment and Plan Governance

CloudNett remains committed to responding fully and within 24 hours to call traceback requests from the Commission, law enforcement, and the traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers initiating calls.

CloudNett has not been prohibited from filing a certification in the Robocall Mitigation Database.

CloudNett reviews and maintains its robocall mitigation program and updates it within 10 business days when filing information, services, traffic patterns, or risk controls change.

Point of Contact:

Josh Cockley
President, CloudNett
717-633-8800

Josh.cockley@CloudNett.net

This program demonstrates CloudNett's commitment to protecting consumers, upholding industry standards, and contributing to the elimination of illegal robocalls.