

Robocall Mitigation Program Description

Filing Entity: Reach Networks LLC

Submission Date: January 20, 2026

Robocall Mitigation Contact:

Robbie Simmons

Email: robbie@reach-networks.com

Phone: 765-529-8606 x106

I. Executive Summary

Reach Networks LLC ("Reach Networks") is a full-service Managed Service Provider (MSP) that provides voice services exclusively to business customers with whom we maintain comprehensive IT management relationships. We utilize CoreDial's voice platform, which has fully implemented the STIR/SHAKEN authentication framework. This document describes our robocall mitigation program in compliance with 47 CFR § 64.6305.

II. Business Model and Customer Base

Reach Networks operates as a comprehensive MSP, providing integrated IT services including servers, computers, networking, security, cameras, and voice services. Our voice services are provided exclusively to existing managed IT clients, ensuring we have detailed knowledge of our customers' legitimate business operations.

We do not offer standalone voice services to unknown parties. All voice service customers are businesses for whom we already provide other managed IT services, giving us direct insight into their operations, business legitimacy, and calling patterns.

III. STIR/SHAKEN Implementation

Reach Networks has fully implemented STIR/SHAKEN authentication through our carrier, CoreDial/SkySwitch. CoreDial has submitted its own filing in the Robocall Mitigation Database and maintains complete STIR/SHAKEN implementation across its network.

Technical Implementation:

- **Attestation Level A:** Applied to calls where the Caller ID is a phone number purchased directly from CoreDial
- **Attestation Level B:** Applied to SIP trunks that utilize passthrough/custom caller ID or forwarded calls

All calls originated by Reach Networks traverse CoreDial's STIR/SHAKEN-compliant network infrastructure, ensuring complete coverage and authentication of caller identification information.

IV. Reasonable Steps to Avoid Originating Illegal Robocalls

A. Real-Time Traffic Monitoring

CoreDial's platform employs comprehensive monitoring software that analyzes outbound voice traffic in real-time to prevent the origination of illegal robocalls. This system provides:

- Detailed reporting identifying suspected illegal robocalls
- Automated alerts when calls originate from invalid or unallocated numbers
- Immediate notification to Reach Networks of any suspicious calling patterns

B. Call Analytics and Pattern Recognition

Reach Networks maintains access to CoreDial's reporting and analytics systems, which provide:

- Complete call volume analysis and trending
- Full call logs for both inbound and outbound traffic
- Pattern detection for unusual calling behavior
- Real-time visibility into customer calling activity

We actively review these analytics to identify any anomalous calling patterns that could indicate illegal robocalling activity.

C. Investigation and Response Procedures

Upon identification of any flagged calls or suspicious activity, Reach Networks commits to:

- Immediately investigate the identified traffic to determine legitimacy
- Contact the customer to understand the nature of the calling activity
- Issue warnings to customers engaging in questionable practices
- Terminate service for customers determined to be originating illegal robocalls

V. Know Your Customer Procedures

A. Customer Verification and Legitimacy

Reach Networks employs a unique and highly effective "Know Your Customer" approach based on our comprehensive MSP service model:

- **Pre-existing Business Relationships:** We provide voice services exclusively to customers with whom we already maintain managed IT service relationships
- **On-site Presence:** Our technicians regularly visit customer locations to manage servers, computers, networking equipment, security systems, and cameras
- **Direct Knowledge:** Through our comprehensive IT management role, we have detailed knowledge of our customers' business operations, physical locations, and legitimate business activities
- **Ongoing Monitoring:** Our continuous IT management activities provide constant visibility into customer operations and any changes in business practices

B. Customer Acceptance Policy

We do not accept voice service customers who are not also managed IT clients. This policy ensures that:

- We maintain direct relationships with all voice service customers

- We have verified the legitimacy of all customer businesses through our comprehensive IT services
- We can identify and address any suspicious activities immediately
- We minimize the risk of providing services to potential bad actors

C. Contractual Provisions

While we operate on a month-to-month billing basis, our service provision includes implicit agreement to acceptable use policies. Customers understand that:

- Voice services must be used only for legitimate business purposes
- Illegal robocalling and caller ID spoofing are prohibited
- Services may be terminated immediately for violations
- Customers must cooperate with any traceback or investigative requests

VI. Historical Performance and Compliance

Reach Networks has maintained an exemplary record of compliance:

- **No Customer Complaints:** We have not received complaints regarding illegal robocalls from any source
- **No Enforcement Actions:** We have never been subject to FCC enforcement actions, investigations, or penalties
- **No Service Terminations:** We have never needed to terminate service due to illegal robocalling activity
- **Proactive Spam List Management:** We have successfully assisted legitimate customers (primarily automotive dealerships) in resolving spam listing issues with downstream carriers when their legitimate business calls were incorrectly flagged

Our business model of serving only established, managed IT clients has proven highly effective in preventing any illegal robocalling activity from originating on our network.

VII. Upstream Provider Knowledge

Reach Networks utilizes a single, trusted upstream voice service provider:

- **Provider:** CoreDial/SkySwitch
- **Relationship:** Long-term partnership with established compliance record
- **RMD Status:** CoreDial has submitted its filing in the Robocall Mitigation Database
- **STIR/SHAKEN Status:** Fully implemented across CoreDial's entire network
- **Monitoring:** We verify CoreDial's continued compliance and STIR/SHAKEN implementation status

VIII. Third-Party Analytics and Blocking

Reach Networks relies on CoreDial's built-in monitoring, analytics, and blocking systems rather than third-party vendors. CoreDial's platform includes:

- Real-time traffic analysis and pattern detection

- Automated identification of invalid and unallocated numbers
- Comprehensive call logging and reporting capabilities
- Integration with industry traceback systems

IX. Traceback Response Commitment

Reach Networks commits to responding fully and within 24 hours to all traceback requests from:

- The Federal Communications Commission (FCC)
- Federal, state, and local law enforcement agencies
- The Industry Traceback Consortium

Our response procedures include:

- Immediate acknowledgment of traceback requests
- Comprehensive investigation of identified traffic
- Full disclosure of relevant call records and customer information
- Cooperation in identifying the source and nature of flagged calls
- Immediate action to block or terminate services as appropriate

Contact for traceback requests:

Robbie Simmons

Email: robbie@reach-networks.com

Phone: 765-529-8606 x106

X. Cooperation with Investigative Entities

Reach Networks commits to full cooperation with the FCC, law enforcement agencies, and the Industry Traceback Consortium in investigating and stopping illegal robocallers. This cooperation includes:

- Providing complete call detail records upon request
- Sharing customer information as legally permitted and required
- Participating in investigations and enforcement proceedings
- Implementing recommended blocking or mitigation measures
- Testifying or providing evidence as needed
- Taking immediate action to terminate services to identified bad actors

XI. Ongoing Compliance and Program Updates

Reach Networks commits to maintaining and continuously improving our robocall mitigation program through:

- Regular review of FCC rules and guidance
- Monitoring of industry best practices and emerging threats
- Coordination with CoreDial regarding platform updates and enhancements
- Annual review and update of this mitigation program

- Prompt updates to our Robocall Mitigation Database filing as required
- Training and awareness for staff regarding robocall mitigation obligations

XII. Certifications

Reach Networks LLC hereby certifies that:

- All calls originated on our network are subject to this robocall mitigation program
- We have implemented reasonable steps to avoid originating illegal robocall traffic
- We commit to responding fully and within 24 hours to all traceback requests
- We commit to cooperating with investigative entities in stopping illegal robocallers
- All calls we originate traverse CoreDial's fully STIR/SHAKEN-compliant network
- We have not been subject to any prior FCC enforcement action related to robocalls
- We have not been prohibited from filing in the Robocall Mitigation Database
- This mitigation program description is accurate and complete

Submitted by:

Robbie Simmons
Reach Networks LLC
robbie@reach-networks.com
765-529-8606 x106

Submission Date: January 20, 2026