

Robocall Mitigation Program Description

PEREGRINE CONSULTING CORP

This Robocall Mitigation Program Description ("RMD Plan") is submitted by PEREGRINE CONSULTING CORP in accordance with FCC requirements under 47 CFR §64.6305. The company certifies that all voice traffic originating on its network is subject to robocall mitigation procedures designed to prevent unlawful robocalls, caller ID spoofing, and fraudulent telecommunications activity.

Business Name	PEREGRINE CONSULTING CORP
FCC Registration Number (FRN)	0038413985
Business Address	2700 N. Military Trail, Ste 100, Boca Raton, FL 33431
Foreign Voice Service Provider	No
Operating Company Number (OCN)	Not Assigned
Primary Contact	Amber Norwood
Contact Title	Senior VoIP Network Engineer
Contact Department	Network Operations
Contact Telephone	561-594-5385
Contact Email	amber.norwood@peregrineconsulting.org

1. STIR/SHAKEN Implementation

PEREGRINE CONSULTING CORP certifies that it has fully implemented the STIR/SHAKEN authentication framework across its IP-based voice network in compliance with FCC regulations. The company authenticates outbound calls where technically feasible and validates inbound caller identity information to reduce spoofed and unlawful traffic.

2. Traffic Monitoring and Analytics

The company utilizes monitoring systems, SIP signaling analysis, fraud detection mechanisms, and traffic pattern analytics to identify suspicious calling behavior. Calls exhibiting abnormal duration, velocity, ASR/ACD anomalies, invalid CLI presentation, or high complaint ratios may be blocked, flagged, or investigated.

3. Know Your Customer (KYC) Procedures

All customers are subject to onboarding verification procedures including business identity verification, validation of contact information, intended traffic use review, and fraud risk assessment. Customers engaging in unlawful robocalling, spoofing, phishing, scam campaigns, or traceback non-compliance are subject to immediate suspension or termination.

4. Traceback Cooperation

PEREGRINE CONSULTING CORP commits to responding promptly to traceback requests from the FCC, law enforcement agencies, industry traceback consortiums, and authorized partners. The company maintains call detail records and routing logs necessary to assist investigations into illegal robocall traffic.

5. Network Security Controls

The network infrastructure is protected using SBC-based filtering, IP authentication policies, rate limiting, ACL enforcement, fraud detection systems, and real-time monitoring controls. Unauthorized SIP traffic and malformed signaling attempts are blocked at the edge network layer.

6. Record Retention

Relevant customer onboarding records, traceback correspondence, traffic monitoring data, and mitigation logs are retained in accordance with applicable FCC and telecommunications compliance requirements.

Certification

PEREGRINE CONSULTING CORP certifies under penalty of perjury that the information contained in this Robocall Mitigation Program Description is true and accurate to the best of its knowledge and complies with applicable FCC robocall mitigation requirements.

Authorized Signatory	Daniel Whitmore
Date	05/13/2026