

The Partnership for Hope — FCC Robocall Mitigation Database (RMD) Program

Date: February 2026

Entity Type: Voice Service Provider (VoIP Reseller)

Underlying Platform: SkySwitch (white-label UCaaS/VoIP)

Robocall Compliance Officer	David Matthew Seaman, Executive Director
Email	daveseaman@partnershipforhope.org
Phone	717-545-7555, 717-609-7527

1) FCC RMD Program Overview

Robocall Mitigation Program Summary

The Partnership for Hope ("TPFH") provides unified communications and voice services to nonprofit organizations using the SkySwitch white label platform. As a voice service provider, we comply with 47 CFR § 64.6305, which requires all voice service providers to implement an appropriate robocall mitigation program and respond to traceback requests within 24 hours.

TPFH ensures STIR/SHAKEN caller ID authentication via our upstream provider, SkySwitch, consistent with 47 CFR § 64.6301. SkySwitch applies **A attestation** to calls using SkySwitch assigned DIDs and **B attestation** to BYOT numbers, per its published policies. While TPFH is launching services and presently has no SkySwitch assigned DIDs, our mitigation program is fully in place and will apply to any traffic we originate; BYOT traffic (if enabled) will receive the appropriate attestation. For any traffic segments not authenticated end to end, TPFH applies layered mitigation: customer identity verification (KYC/KYB), number authorization checks, traffic analytics, high risk pattern detection, call blocking/labeling for suspected illegal calls, and rapid remediation procedures.

TPFH commits to: (1) responding fully to all traceback requests within 24 hours; (2) blocking illegal or suspicious traffic upon FCC notification and identifying upstream providers as required; and (3) implementing "know your upstream provider" procedures, including verification that SkySwitch maintains an active RMD filing.

We maintain records of KYC/KYB checks, number authorization, attestation metadata, traffic analytics alerts, traceback responses, and mitigation actions for at least one year. Our written mitigation program is available upon request.

Primary Contact / Robocall Compliance Officer:

David Matthew Seaman — Executive Director / Robocall Compliance Officer

Email: daveseaman@partnershipforhope.org | Phone: 717-545-7555

2) Full Robocall Mitigation Program

Overview

TPFH prohibits the origination or facilitation of illegal robocalls and maintains a mitigation program meeting FCC requirements under 47 CFR § 64.6305. This includes reasonable steps to avoid originating illegal robocall traffic and a mandatory 24 hour traceback response obligation.

STIR/SHAKEN Implementation (via SkySwitch)

SkySwitch signs calls with A attestation for SkySwitch assigned DIDs and B attestation for BYOT numbers. Invalid/unallocated numbers are flagged and prevented from egress where required. STIR/SHAKEN implementation is provided by SkySwitch, satisfying the caller ID authentication obligation in 47 CFR § 64.6301.

Know Your Customer (KYC) & Number Authorization

We verify nonprofit identity (EIN, registration), authorized representatives, ownership/authorization for all outbound TNs (SkySwitch DIDs or BYOT with LOA), and expected call patterns; we bind TNs to specific customers or campaigns.

Traffic Monitoring & Analytics

We monitor short duration spikes, calls per minute, sequential dialing patterns, high AMD/no answer rates, geographic anomalies, and labeling/consumer complaints. Suspicious traffic triggers review, throttling, number quarantine, or suspension.

Call Blocking & Mandatory FCC Blocking

We block traffic determined to be highly likely illegal and block upon FCC notification; we identify upstream providers as required.

24 Hour Traceback Response

We respond to all traceback requests from the FCC, law enforcement, or the Industry Traceback Group within 24 hours.

Know Your Upstream Provider (KYUP)

We verify SkySwitch's RMD status and compliance and refuse traffic from any upstream lacking an RMD filing.

Recordkeeping (≥ 1 Year)

We maintain KYC files, LOAs/number proofs, attestation metadata, analytics alerts, traceback responses, blocking actions, and RMD filings/updates.

Enforcement & Customer Terms

We immediately suspend or terminate customers engaged in illegal calling and report events as required. We require compliance with TCPA/state rules for dialer usage (consent/time of day).

3) Operational SOPs

New Customer Provisioning

- Collect EIN, registration, authorized contact; verify nonprofit status.
- Validate ownership/authorization for all outbound TNs (SkySwitch DID vs. BYOT).
- Assign CNAM/brand verification where supported.
- Set analytics thresholds (calls/minute, short duration ratio).
- Document expected traffic patterns and bind TNs to accounts/campaigns.

Alert/Incident Response

- Pause affected TNs/campaigns when an alert triggers.
- Investigate (CDRs, SIP logs, scripts, consent records).
- Remediate: unblock with tuning or block/suspend and notify customer.
- If traceback request: respond within 24 hours with full path and remediation.
- Record the incident; update thresholds as needed.

4) RMD Compliance Checklist

- ☐ FRN active and correct in CORES.
- ☐ RMD filing completed with program summary and contact info.
- ☐ 24-hour traceback SOP implemented and tested.
- ☐ Blocking on notice SOP implemented.
- ☐ Know your upstream procedures documented; SkySwitch RMD status verified.
- ☐ Number inventory governance in place (no SkySwitch DIDs at launch; update as issued).
- ☐ Staff trained; annual review scheduled.

Regulatory basis: 47 CFR § 64.6301 (Caller ID Authentication); 47 CFR § 64.6305 (Robocall Mitigation & Certification); 2024 FCC updates on 24 hour traceback, KYUP, and blocking on notice.