

ROBOCALL MITIGATION PLAN (RMP) Filing Entity: Oak Cyber LLC d/b/a Fraternity Communications **FCC CORES FRN:** 0038726634 **Filing Category:** Voice Service Provider Serving End-Users **STIR/SHAKEN Certification Option:** Option 3 – No STIR/SHAKEN Implementation (Non-Facilities-Based Provider Exemption pursuant to 47 CFR § 64.6304) **Date of Adoption / Effective Date:** July 31, 2026

1. EXECUTIVE SUMMARY & REGULATORY CLASSIFICATION Oak Cyber LLC d/b/a Fraternity Communications (the "Company") provides managed cloud telephony infrastructure and pre-configured hardware endpoints to enterprise, SMB, and commercial multi-dwelling unit (MDU) clients throughout the United States. This Robocall Mitigation Plan governs all service tiers and product lines deployed under the Company's operations.

The Company elects Option 3 (No STIR/SHAKEN Implementation) and claims the Non-Facilities-Based Provider Exemption (47 CFR § 64.6304) on the following operational grounds:

1. The Company is a non-facilities-based managed service provider and does not own or operate underlying Class 4/5 telephone carrier switches, Session Border Controllers (SBCs), or SIP signaling infrastructure capable of cryptographically signing call headers with its own Service Provider Code (SPC) token.
2. All originating voice traffic generated by the Company's end-users is routed exclusively through our FCC-registered originating carrier of record (VoIP.ms and its underlying STIR/SHAKEN-compliant carrier partners), which cryptographically signs originating SIP calls with A-Attestation prior to entering the Public Switched Telephone Network (PSTN).
3. All originating traffic carried on the Company's network is subject to the rigorous, multi-layered Know-Your-Customer (KYC), endpoint-lockdown, and robocall mitigation controls documented herein.

2. KNOW-YOUR-CUSTOMER (KYC) ONBOARDING & VETTING PROCEDURES The Company enforces strict Know-Your-Customer (KYC) onboarding protocols to verify the legal identity, physical location, and legitimate communications intent of every organization prior to provisioning telephony resources or originating access.

We do not provide instant, unverified online activation, nor do we resell open SIP trunks to unverified third parties or wholesale brokers. Our KYC vetting workflow requires:

2.1 Entity & Tax Identification Verification Before service activation, every prospective commercial client must submit authenticated documentation confirming its legal standing:

- **Government Tax Identification:** A copy of the organization's IRS Form SS-4, EIN assignment letter, or Form W-9 verifying their Employer Identification Number (EIN).
- **Corporate Registration:** Proof of active legal registration (e.g., Articles of Organization, State Certificate of Good Standing, or equivalent corporate charter acknowledgment).

2.2 Authorized Representative Authentication The Company authenticates the natural persons responsible for the account:

- **Representative Validation:** We collect and verify the full legal name, title (e.g., Chief Executive Officer, Treasurer, or Authorized Trustee), corporate email address, and verified callback telephone number of the authorized corporate officer.
- **Identity Documents:** When required for fraud deterrence, government-issued photo identification (Driver's License or Passport) is validated against the authorized signatory.

2.3 Physical Address & E911 Demarcation Verification Every telephone line and Direct Inward Dialing (DID) number provisioned by the Company is mapped to a verified, physical commercial or MDU address. Validated E911 address registration is a mandatory prerequisite prior to hardware dispatch.

3. HARDWARE & ENDPOINT LOCKDOWN MODEL Unlike general VoIP providers that allow end-users to register arbitrary softphones, PBX servers, or high-volume dialers, the Company operates a strictly managed Hardware-As-A-Service (HaaS) Endpoint Lockdown Model:

- **Centrally Managed Hardware Only:** End-users originate calls exclusively through pre-configured Analog Telephone Adapters (ATAs) and SIP gateways staged and programmed at the Company's staging facility.
- **Zero User-Accessible Credentials:** SIP subaccount credentials (SIP Server, SIP User ID, and high-entropy alphanumeric passwords) are cryptographically generated, encrypted, and pushed directly to hardware endpoints via secure cloud provisioning (e.g., GDMS). End-users do not have access to raw SIP credentials and cannot load the Company's trunks onto third-party dialing software.
- **Fixed-Port Call Routing:** Provisioned hardware ports are dedicated to specific physical applications, including standard commercial common-area handsets, facility access control intercoms, and automated reception routing.
- **Channel & Rate Limiting:** All client subaccounts are configured with strict channel limits (typically 2 to 4 concurrent channels per device) to physically prevent call-blasting or high-volume call origination.

4. PROHIBITED TRAFFIC POLICY & ACCEPTABLE USE RULES The Company maintains a zero-tolerance policy for illegal, fraudulent, or high-volume automated telephony traffic. Our Terms of Service and mandatory Acceptable Use Policy (AUP) explicitly prohibit:

- **Autodialing & Predictive Dialers:** Using the Company's lines for automated dialing, robocasting, artificial/prerecorded voice blasting, or predictive dialing campaigns.
- **Telemarketing & Solicitation:** Originating unsolicited commercial telemarketing, political blasting, or charitable phone solicitations.
- **Caller ID Spoofing:** Originating calls with false, misleading, or unauthorized Caller ID (CNAM/ANI) information, including impersonating corporate officers, financial institutions, or government agencies.
- **Traffic Resale:** Sub-reselling, bridging, or sharing the Company's SIP lines with unverified external entities.

Violation of these policies triggers immediate, unilateral service suspension without notice and forfeiture of provisioned equipment.

5. UPSTREAM CARRIER VETTING & CALL AUTHENTICATION The Company originates 100% of its voice traffic through reputable, FCC-registered upstream carriers that maintain active filings in the Robocall Mitigation Database and comply with STIR/SHAKEN authentication mandates:

- **Primary Originating Upstream:** VoIP.ms (Swiftkick Communications Inc. / associated operating entities).
- **Authentication Assurance:** The Company transmits accurate, verified calling party numbers (DIDs assigned to the commercial client) on all outbound calls. Our upstream carrier partners cryptographically sign these calls with STIR/SHAKEN A-Attestation (or highest applicable attestation level) prior to routing across the public network.
- **Upstream Monitoring:** The Company regularly verifies that all upstream carriers we interconnect with remain in good standing in the FCC Robocall Mitigation Database.

6. TRACEBACK COMMITMENT & LAW ENFORCEMENT COOPERATION The Company commits to full, proactive cooperation with industry and legal authorities to identify, investigate, and stop illegal robocallers:

1. **24-Hour Traceback Responsiveness:** The Company commits to respond fully and accurately to all traceback requests from the FCC, law enforcement agencies, and the industry traceback consortium (the Industry Traceback Group / ITG) within twenty-four (24) hours of receipt.
2. **Dedicated Compliance Officer:** The Company maintains an assigned Robocall Mitigation Officer reachable by regulatory and traceback authorities:
 - **Name / Title:** Ben Venable, Director of Compliance
 - **Company:** Oak Cyber LLC d/b/a Fraternity Communications
 - **Business Address:** 9418 Colleton Way, Montgomery, AL 36117
 - **Compliance Email:** fcccompliance@[yourdomain].com
3. **Data Preservation:** The Company maintains complete call-detail records (CDRs), hardware MAC address logs, and KYC customer identification files to ensure rapid trace-to-source attribution.

7. TRAFFIC MONITORING, INCIDENT RESPONSE & TERMINATION PROCEDURE To prevent abuse on our network, the Company executes ongoing traffic monitoring and an immediate incident remediation protocol:

- **Automated Anomaly Detection:** We monitor account usage dashboards for abnormal call origination metrics, including short-duration call spikes, unusual after-hours call volumes, or attempts to dial high-frequency destinations.
- **Immediate Suspension Protocol:** If the Company detects suspicious calling patterns—or receives a verified traceback alert, fraud report, or notice of illegal spoofing—our engineering team immediately executes the following remediation sequence:

1. **Instant Subaccount Lock:** The offending SIP subaccount is disabled via cloud API within minutes of detection, blocking all outbound call origination.
2. **Hardware De-Registration:** The physical ATA/gateway endpoint is locked and de-registered remotely via secure cloud management.
3. **Investigation & Audit:** The Company initiates an investigation with the client's authorized representative. If illegal robocalling or willful spoofing is confirmed, the customer's contract is permanently terminated, and findings are preserved for regulatory authorities.

8. ONGOING COMPLIANCE & DATABASE MAINTENANCE The Company certifies that it will maintain its robocall mitigation compliance through the following statutory requirements:

- **10-Business-Day Update Rule:** Pursuant to 47 CFR § 64.6305, the Company will update its Robocall Mitigation Database filing within ten (10) business days of any material change to our legal name, contact person, ownership, or robocall mitigation practices.
- **Annual Recertification:** The Company commits to performing annual recertification of this Robocall Mitigation Plan and our FCC CORES registrations in accordance with Commission deadlines.

CERTIFICATION & SIGNATURE I, Ben Venable, certify under penalty of perjury that I am an authorized officer of Oak Cyber LLC d/b/a Fraternity Communications, that I have examined this Robocall Mitigation Plan, and that to the best of my knowledge, information, and belief, all statements of fact contained herein are true, accurate, and correct.

Ben Venable VP of Regulatory Affairs, Oak Cyber LLC d/b/a Fraternity Communications July 31, 2026