

ROBOCALL MITIGATION PLAN (RMP)

Filed in the FCC Robocall Mitigation Database (RMD)

Company Name: My Vet Hub Inc

FRN: 0038144614

Service Type: VoIP Reseller

Service Type: Interconnected VoIP Reseller (SkySwitch Cloud PBX)

Date: 03/20/2026

1. PURPOSE AND REGULATORY COMPLIANCE

This Robocall Mitigation Plan ("Plan") is adopted in compliance with the Communications Act of 1934, as amended, and applicable Federal Communications Commission ("FCC") regulations, including but not limited to 47 CFR § 64.6300 et seq.

My Vet Hub Inc("Company") affirms that it has implemented reasonable and effective measures to prevent the origination and transmission of illegal robocalls and unlawful messaging traffic.

2. SERVICE DESCRIPTION

The Company operates as a reseller of hosted VoIP and messaging services utilizing the SkySwitch Cloud PBX platform. The Company does not directly control underlying transmission facilities and relies on upstream providers for network-level authentication and routing.

3. STIR/SHAKEN RELIANCE

The Company relies on upstream providers, including SkySwitch and its carrier partners, for implementation of STIR/SHAKEN protocols. The Company shall ensure that all

originating customers are properly vetted such that upstream attestation is accurate and not misleading.

3.1 STIR/SHAKEN STATUS

The Company certifies that it has NOT implemented the STIR/SHAKEN authentication framework on any portion of its network. This filing reflects Option 3 (No STIR/SHAKEN Implementation) as defined in 47 CFR § 64.6305.

3.2 BASIS FOR NON-IMPLEMENTATION:

- The Company is a reseller of VoIP services and does not own or control the underlying network infrastructure necessary to implement STIR/SHAKEN call authentication.
- The Company resells VoIP services through Skyswitch, a white-label wholesale VoIP provider. Skyswitch, as the facilities-based carrier controlling the IP network infrastructure, bears the STIR/SHAKEN implementation obligation under FCC rules.
- Pursuant to the FCC's First Caller ID Authentication Report and Order (35 FCC Rcd 3241, para. 40) and the Eighth Caller ID Authentication Report and Order (FCC 24-120), providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN are exempt from its implementation requirements.

3.3 ROBOCALL MITIGATION PROGRAM

Although the Company is exempt from STIR/SHAKEN implementation, The Company maintains a robocall mitigation program consistent with 47 CFR § 64.6305(a). The following measures describe The Company's reasonable steps to avoid originating illegal robocall traffic.

4. CUSTOMER DUE DILIGENCE (KYC)

The Company implements commercially reasonable Know Your Customer ("KYC") procedures, including:

- Verification of customer identity and business legitimacy
- Collection of government-issued identification and/or corporate registration documents
- Validation of physical address and contact information

- Risk-based assessment for high-volume or high-risk use cases

The Company reserves the right to deny, suspend, or terminate service where customer identity cannot be verified or presents elevated risk.

5. CALLER ID AUTHENTICATION AND SPOOFING PREVENTION

The Company enforces strict prohibitions on caller ID spoofing. Customers may only originate calls using:

- Telephone numbers assigned by the Company; or
- Numbers for which the customer provides verifiable proof of ownership or authorization.

Any violation shall result in immediate suspension or termination of services.

6.1 TRAFFIC MONITORING AND FRAUD DETECTION

The Company employs ongoing monitoring of call and messaging traffic, including but not limited to:

- Call Detail Record (CDR) analysis
- Detection of abnormal traffic patterns
- Monitoring of answer-seizure ratios (ASR) and call durations
- Review of customer complaint data and carrier feedback

6.2 ACCEPTABLE USE POLICY

The Company maintains the right to block, suspend, or investigate any traffic deemed suspicious.

The Company prohibits the following uses of its voice services:

- Origination of illegal robocalls or automated calls in violation of the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227, or the FCC's implementing regulations.
- Caller ID spoofing or falsification of caller ID information in violation of the Truth in Caller ID Act, 47 U.S.C. § 227b.
- Transmission of calls that have been identified as illegal, fraudulent, or the subject of a traceback request by the FCC, law enforcement, or the industry traceback consortium.

Violations of these prohibitions are grounds for immediate service suspension and termination.

7. ENFORCEMENT AND MITIGATION ACTIONS

Upon detection of suspected illegal activity, the Company shall take immediate remedial actions, including:

- Suspension or restriction of services
- Termination of customer accounts
- Blocking of originating traffic
- Notification to upstream providers and/or relevant authorities

8. A2P 10DLC COMPLIANCE (LEGAL STANDARD)

The Company enforces strict compliance with all applicable A2P 10DLC regulations and carrier requirements, including:

a. Mandatory Registration:

All customers must register their brand and messaging campaigns with The Campaign Registry (TCR) prior to sending A2P traffic.

b. Consent and Opt-In Requirements:

Customers must obtain express, informed consent from end users prior to initiating messaging. Consent must be documented and auditable.

c. Opt-Out Compliance:

Customers must honor all opt-out requests, including STOP, HELP, and carrier-mandated keywords, in real time.

d. Content Compliance:

The Company strictly prohibits transmission of unlawful, deceptive, or prohibited content, including but not limited to SHAFT categories and any content violating TCPA or CTIA guidelines.

e. Monitoring and Enforcement:

The Company monitors messaging throughput, complaint rates, and carrier feedback. Non-compliant campaigns shall be immediately suspended or terminated.

9. TRACEBACK COOPERATION

The Company agrees to fully cooperate with traceback requests from the Industry Traceback Group (ITG), FCC, and law enforcement agencies, and shall provide timely and accurate responses.

10. RECORD RETENTION

The Company retains relevant records, including customer onboarding documentation, traffic data, and complaint logs, for a minimum period of twelve (12) to twenty-four (24) months.

11. UPSTREAM RELIANCE AND ESCALATION

The Company coordinates with SkySwitch and upstream carriers to ensure mitigation of illegal traffic and shall promptly escalate any identified threats or violations.

12. COMPLIANCE GOVERNANCE

The Company maintains internal compliance procedures and training programs to ensure adherence to FCC rules and industry best practices.

13. CONTACT INFORMATION

Compliance Officer: [Full Name]

Title: [Title]

Email: [Email Address]

Phone: [Phone Number]

14. CERTIFICATION

Pursuant to 47 CFR § 1.16, I certify under penalty of perjury that:

- The foregoing information is true and correct to the best of my knowledge;
- The Company has implemented the robocall mitigation practices described herein;
- The Company will continue to comply with all applicable FCC rules and regulations.

Authorized Representative:

Name: Dharm Singh

Title: Director

Signature: *Dharm Singh*

Date: 03/26/2020