

Mobert Marine LLC
(dba Sea-Tech Systems)

7001 Seaview Ave NW, #160-485
Seattle, WA 98117

Robocall Mitigation Program Description

(For FCC Robocall Mitigation Database Filing – 47 CFR § 64.6305)

1. Company Overview

Mobert Marine LLC dba Sea-Tech Systems is a small consulting first maritime service reseller purchasing wholesale VoIP services from VoIP.ms. The company provides VoIP services exclusively to its own affiliated companies and a limited number of known business and individual users personally known to the company. Service usage is low-volume and intended for ordinary business or personal communications and usually bundled with other services such as Internet or satellite data. The company does not provide open retail access of voice services to the public and does not permit automated outbound calling platforms. The company does not originate, carry, or process robocall campaigns and does not provide services to telemarketers, call centers, or mass-dialing operations.

2. Reasonable Steps to Avoid Origination, Carrying, or Processing of Illegal Robocalls

A. Restricted Customer Base

Services are provided only to the company's own internal operations or a small number of known and vetted individuals or businesses. No anonymous, public, or automated signups are permitted. No wholesale downstream resellers are allowed.

B. Customer Vetting and Control Measures

The company takes affirmative and effective measures to prevent new and renewing customers from originating illegal calls. All users are personally known to the company. High-volume telemarketing or automated dialer use is not permitted. Customers are prohibited from originating illegal robocalls, unlawfully spoofing caller ID, or violating TCPA or FCC rules. The company retains sole administrative control over SIP credentials, DID provisioning, and call routing configurations. Suspicious or unlawful activity results in immediate suspension or termination.

C. Technical Safeguards

Strong SIP authentication passwords are required. SIP credentials are not publicly shared. Administrative access to VoIP.ms accounts is restricted. Call logs are regularly reviewed for unusual activity. Usage volumes are monitored and remain very low.

D. Monitoring and Traffic Review

The company regularly reviews call detail records (CDRs) and monitors for abnormal call volume spikes, short-duration call patterns, or repetitive outbound patterns. If anomalous behavior is detected, the company will suspend affected credentials, investigate records, notify the upstream provider if appropriate, and terminate service if illegal activity is confirmed.

3. Know-Your-Upstream Provider Procedures

The company obtains wholesale VoIP service exclusively from VoIP.ms and maintains a direct business relationship. It operates under VoIP.ms terms of service and compliance policies and does not accept traffic from unknown upstream providers. The company is not a gateway provider and does not carry third-party upstream traffic.

4. Call Analytics and Blocking Systems

The company relies on upstream call analytics, fraud detection, and mitigation systems implemented by VoIP.ms and its carrier partners. Internal monitoring of call logs and usage patterns is conducted regularly. Due to small scale and low traffic volume, no independent analytics engine is operated.

5. STIR/SHAKEN

As a reseller, the company relies on VoIP.ms and its underlying carriers for STIR/SHAKEN implementation where applicable and does not directly operate signaling infrastructure requiring independent authentication.

6. Response Procedures for Illegal Traffic

If illegal robocall activity is detected, the company will immediately suspend the originating SIP credentials, investigate call detail records, terminate the customer if appropriate, cooperate with its upstream provider, and implement corrective measures to prevent recurrence.

7. Statement of Compliance

The company affirms that it has implemented reasonable and effective steps to prevent the origination of illegal robocalls. It provides service only to a limited, known customer base, prohibits automated robocall campaigns, monitors traffic, maintains administrative control over all lines, and relies on upstream carrier mitigation systems. This plan will be updated as necessary to remain compliant with FCC regulations.