

SEAWOLF TECHNOLOGIES, INC.

ROBOCALL MITIGATION PLAN

Updated September 2026 - Rev. 4a

I. Background

The Federal Communications Commission ("FCC" or "Commission") has adopted rules requiring voice service providers, including Seawolf Technologies, Inc. ("Seawolf"), to file certifications and robocall mitigation plans in the FCC's Robocall Mitigation Database ("RMD"). See 47 C.F.R. § 64.6305.

The FCC requires voice service providers to certify in the RMD regarding implementation of the STIR/SHAKEN caller ID authentication framework and to maintain a robocall mitigation program consistent with the Commission's rules. Seawolf's program includes reasonable steps designed to avoid originating illegal robocall traffic, a commitment to respond within 24 hours to traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperation with such entities in investigating and stopping illegal robocallers that use Seawolf's service to originate calls.

Seawolf's mitigation efforts focus on potentially unlawful calling activity, including calls that may violate 47 U.S.C. § 227(b), as applicable, and the Truth in Caller ID Act, 47 U.S.C. § 227(e).

This document describes Seawolf's current robocall mitigation practices, including its Know Your Customer procedures, contractual restrictions, STIR/SHAKEN implementation, network monitoring, and traceback response commitments.

II. Seawolf's Know Your Customer ("KYC") Standards

Seawolf is a voice service provider focused on business-user and wholesale voice communications services. Seawolf applies KYC criteria to current and prospective customers and uses commercially reasonable procedures to verify customer identity and business legitimacy.

As part of customer onboarding, Seawolf requires customers, as applicable, to complete a KYC questionnaire, provide a USF Exemption Certificate for carrier customers, and enter into a formal written contract. Seawolf collects and, as appropriate, verifies customer-identifying information, including:

- Customer business name and entity type;
- State or country of incorporation;
- Physical business location;
- Main, technical, and compliance contact information;
- Trade and/or bank references, as appropriate;
- Federal tax identification number;
- FCC Form 499 Filer ID and FRN, as applicable;
- Robocall Mitigation Database filing and STIR/SHAKEN compliance information, as applicable; and
- Company website and/or other customer-facing presence.

Seawolf's verification practices include confirming a carrier customer's reported status in the FCC's Form 499 Filer database and the Commission's Robocall Mitigation Database, conducting internet research regarding the company's reasonably accessible online profile and potential call-usage or complaint history, and, as applicable, checking references with other carrier suppliers and reviewing traceback history. Seawolf also reviews new-account traffic profiles for patterns involving call duration, caller ID usage, answer-seizure ratio (ASR), and other metrics that may help identify traffic-hygiene concerns.

III. Seawolf's Acceptable Use Policy

Seawolf's customers contractually agree to terms and conditions that include compliance with Seawolf's Acceptable Use Policy ("AUP"). Among other things, the AUP prohibits:

- Using Seawolf's services to engage in activities that are illegal, abusive, false, fraudulent, deceptive, or misleading;
- Engaging in unsolicited advertising, marketing, or other unlawful activity, including activity that violates applicable telemarketing, TCPA, FCC, Do Not Call, and calling-time requirements; and
- Creating or using a false identity, forged contact information, unauthorized telephone number, or otherwise attempting to mislead others regarding the identity of the sender or origin of a telephone call, including conduct that violates the Truth in Caller ID Act.

Seawolf's customer agreements authorize Seawolf to suspend and/or terminate services in the event of an AUP violation.

IV. Telephone Number Authorization and STIR/SHAKEN Implementation

Seawolf has implemented the STIR/SHAKEN caller ID authentication framework in its production IP network. Seawolf has completed registration with the STI Policy Administrator ("STI-PA") and has obtained its Service Provider Code ("SPC") authorization. Telonium Communications serves as Seawolf's STI Certification Authority and has issued an STI certificate for Seawolf based on Seawolf's own STI-PA registration and SPC authorization.

Seawolf retains and uses its own private key and performs STIR/SHAKEN authentication and PASSport signing on its own production OpenSIPS infrastructure. Telonium Communications does not sign Seawolf traffic using Telonium's own service-provider identity or certificate.

Seawolf has deployed its STIR/SHAKEN implementation in production and has successfully tested and validated authenticated SIP traffic over production SIP routes with its U.S. termination partners. For traffic authenticated by Seawolf, Seawolf currently generally applies B-level attestation based on its relationship with the originating customer and its authorization to carry the traffic.

Seawolf restricts its end users to making calls only from telephone numbers that Seawolf has assigned to them or numbers for which they have demonstrated a right to use. Seawolf further prohibits unlawful caller ID spoofing and unauthorized prerecorded or artificial-voice calling activity through its contractual restrictions, monitoring efforts, and Acceptable Use Policy.

V. Proactive Network Monitoring

If Seawolf detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing on its network, Seawolf takes prompt action to identify the customer or other party associated with the activity and takes appropriate responsive action. Seawolf uses customer and traffic information, including caller ID usage, call-duration patterns, ASR and other available traffic indicators, together with complaints, traceback information, and other relevant information. Appropriate action may include contacting the customer, restricting or suspending traffic, or terminating service, depending on the circumstances.

VI. Commitment to Timely Traceback Responses and Cooperation

Seawolf commits to respond fully and in a timely manner, within 24 hours, to traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate illegal robocalls. Seawolf will dedicate sufficient resources to provide timely and complete responses, investigate suspicious activity, and take appropriate action.

This Robocall Mitigation Plan reflects Seawolf Technologies, Inc.'s current practices as of September 2026 and supersedes the prior version, including prior descriptions of Seawolf's provider role and STIR/SHAKEN implementation status.