

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Filing Entity	Telimatic LLC
FCC Registration Number (FRN)	0038607891
Provider Type	Voice Service Provider
STIR/SHAKEN Certification Option Selected	Option 3
Robocall Mitigation Point of Contact	Eric Hernaez
Document Effective Date	July 28, 2026

1. Purpose and Scope

Telimatic (“the Company”) submits this Robocall Mitigation Program Description in connection with its certification in the FCC's Robocall Mitigation Database, as required by 47 CFR § 64.6305(a). This document describes the specific, reasonable steps the Company takes to avoid originating illegal robocall traffic on its network, consistent with the Company's certification option selected in the Database.

This program applies to all voice traffic originated by the Company and is reviewed and updated no less than annually, and promptly upon any material change to the Company's network, customer base, or mitigation practices, consistent with the Database's 10-business-day update requirement under 47 CFR § 64.6305(d)(5).

2. STIR/SHAKEN Caller ID Authentication Status

Telimatic has not yet implemented the STIR/SHAKEN authentication framework on any portion of its network. Telimatic is a newly established voice service provider that has not yet completed deployment of the network infrastructure (including an STI-AS and SPC token) necessary to sign calls. Telimatic is in the process of establishing carrier interconnection agreements and building out its network, and will implement STIR/SHAKEN as that infrastructure comes online, updating this certification accordingly.

Extension / Exemption Basis (47 CFR § 64.6305(d)(2)(i))

Telimatic does not claim an extension under 47 CFR § 64.6304. The foregoing statement is provided as the explanation required under 47 CFR § 64.6305(d)(2)(i) of why Telimatic is presently unable to implement STIR/SHAKEN due to its current stage of network build-out.

3. Know-Your-Customer (KYC) Practices

Before provisioning service to a new customer capable of originating traffic on the Company's network, and periodically thereafter, the Company takes the following steps:

- Verifies the identity of the prospective customer, including [legal business name, physical business address, contact person, and government-issued business identification or tax ID], before activating origination service.
- Confirms the customer's intended use case and expected calling patterns (e.g., call volume, destination mix, average call duration) at onboarding.

- Screens new customers against [sanctions lists, known bad-actor lists, and/or the Traceback Consortium's repeat-offender list] prior to activation.
- Requires customers to certify contractually that they will not use the Company's network to transmit illegal, fraudulent, or spoofed robocall traffic (see Section 7).
- Re-verifies customer information and use case [annually / upon contract renewal / upon material change in traffic pattern].
- Monitors for red flags indicating a change in a verified customer's traffic pattern (e.g., sudden volume spikes, abnormally short call durations, high answer-then-hangup ratios) and re-verifies or suspends service where warranted.

4. Know-Your-Upstream-Provider (KYUP) Practices

Before accepting traffic from an upstream voice service provider, and periodically thereafter, the Company:

- Confirms that the upstream provider has a current, active filing in the FCC Robocall Mitigation Database.
- Reviews the upstream provider's RMD certification and robocall mitigation plan for completeness and plausibility.
- Where the upstream provider claims full or partial STIR/SHAKEN implementation, confirms it has obtained an appropriate Service Provider Code (SPC) token.
- Checks whether the upstream provider appears on relevant enforcement, sanctions, or national-security-related lists.
- Reserves contractual and technical rights to suspend or terminate traffic acceptance from any upstream provider found to be a source of illegal robocall traffic.

5. Traffic Monitoring and Call Analytics

- Deploys network-based call analytics to monitor originated and/or carried traffic for patterns consistent with illegal robocalling (e.g., high call volumes to sequential or invalid numbers, abnormally short average call duration, high volumes of unanswered calls).
- Reviews STIR/SHAKEN attestation levels applied to outbound calls and investigates unexplained increases in “gateway” (C-level) or unattested traffic.
- Generates internal alerts when a customer or trunk group exceeds defined volume or pattern thresholds, triggering manual review by the Company's compliance team.
- Maintains the technical capability to suspend or block traffic from a specific customer, trunk, or upstream provider found to be originating illegal traffic, consistent with the Commission's call-blocking safe harbors.

6. Traceback Cooperation

The Company commits to responding fully and within 24 hours to all traceback requests received from the Federal Communications Commission, law enforcement agencies, and the industry traceback consortium (USTelecom Industry Traceback Group), and to cooperate with such entities in investigating and stopping illegal robocallers using the Company's network to originate, carry, or process calls. The Company designates Eric Hernaez as the point of contact for traceback requests, monitored during business hours with after-hours escalation by email to traceback@telimatic.com

7. Contractual and Enforcement Measures

- Customer service agreements prohibit the use of the Company's network to transmit illegal robocalls, illegally spoofed calls, or fraudulent traffic, and reserve the Company's right to immediately suspend service upon reasonable suspicion of such use.
- Repeat or egregious violations result in permanent termination of service and, where appropriate, referral to the FCC, state attorneys general, and/or the industry traceback consortium.

8. Consumer Complaint Handling

- Maintains a process for receiving and investigating complaints regarding suspected illegal robocalls associated with the Company's network, via email and web form.
- Investigates complaints and, where warranted, suspends or terminates the responsible customer's service.
- Tracks complaint volume and trends by customer/trunk group to identify emerging bad actors.

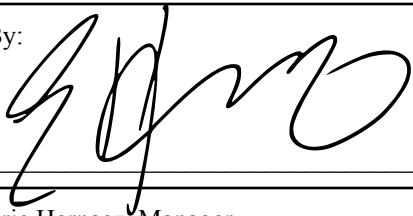
9. Recordkeeping and Recertification

- Telimatic retains KYC/KYUP verification records, traceback correspondence, and complaint investigation records for a minimum of 4 years after the customer relationship ends (or after the record is created, for traceback/complaint records not tied to a specific customer).
- Updates its Robocall Mitigation Database filing within 10 business days of any material change to the information required under 47 CFR § 64.6305, including changes in STIR/SHAKEN implementation status or contact information.
- Re-certifies its Robocall Mitigation Database filing annually, consistent with the Commission's annual recertification requirement.

10. Certification

The undersigned officer certifies that the foregoing accurately describes the Company's robocall mitigation program as actually implemented, and that this program includes reasonable steps to avoid originating, carrying, or processing illegal robocall traffic in compliance with 47 CFR Part 64, Subpart HH.

By:



Eric Hernaez, Manager

July 28, 2026