



Advantec Solutions, Inc.

1820 N Portland Ave

Oklahoma City, OK 73107

405.949.2000 info@advantecsolutions.com <https://advantecsolutions.com>

FCC Registration Number (FRN): 0037485620

Date: September 09, 2025

Robocall Mitigation Program Description

Submitted to: Federal Communications Commission Robocall Mitigation Database

Pursuant to: 47 CFR § 64.6305(d)(ii)-(iii) and RMD Filing Instructions (DA 24-73)

Certification Option: Option 3 – No STIR/SHAKEN Implementation

Provider Type: Voice Service Provider without a STIR/SHAKEN Obligation (Interconnected VoIP Reseller Serving End-Users)

I. Introduction and Provider Overview

Advantec Solutions, Inc. is an S-Corporation incorporated in the State of Oklahoma, registered with the FCC under FRN 0037485620, and operating as a non-facilities-based interconnected Voice over Internet Protocol (VoIP) service provider. We offer VoIP services to business and residential customers primarily in Oklahoma, with plans for limited interstate expansion. As a reseller, we do not own or control underlying network infrastructure (e.g., no IP switches, SIP gateways, or physical facilities); instead, we originate calls by reselling services from FCC-registered upstream carriers (e.g., [Name of Wholesaler, e.g., Bandwidth or Twilio]) that handle transmission and interconnection to the Public Switched Telephone Network (PSTN). This Robocall Mitigation Program Description (RMPD) outlines our comprehensive robocall mitigation program, implemented in compliance with the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act and 47 CFR § 64.6300 et seq. Our program includes reasonable steps to prevent the origination of illegal robocall

traffic on our network and a firm commitment to respond to all traceback requests. As a new provider (operations commencing [insert start date, e.g., September 2025]), we have designed this program to be proactive, scalable, and aligned with industry best practices from the first day of service. We certify under penalty of perjury that:

- All calls we originate are subject to this robocall mitigation program.
- We have not been removed from the Robocall Mitigation Database by Commission action, nor are we prohibited from filing.
- We have fully implemented the program as described herein.

This program will be reviewed and updated annually, or more frequently if our operations change (e.g., expansion to facilities-based services).

Contact for inquiries: James Eggert, CEO, 405.9492000, james@advantec.cc.

II. Exemption from STIR/SHAKEN Implementation

Advantec Solutions, Inc. selects Certification Option 3 (No STIR/SHAKEN Implementation) because we qualify for an exemption from the STIR/SHAKEN authentication framework under 47 CFR § 64.6303(b). This rule exempts non-facilities-based voice service providers that do not have control over the network infrastructure used to originate calls. Explanation of Exemption: As a reseller of VoIP services, we do not own, operate, or control any physical or IP-based network elements (e.g., no Class 5 switches, media gateways, or Session Border Controllers). All call origination, routing, and transmission occur through our upstream wholesale carrier(s), which are responsible for any STIR/SHAKEN signing in the IP portions of their networks. We interface with customers via software APIs and billing platforms but have no direct access to or control over call signaling, authentication tokens, or Secure Telephone Identity Governance Authority (STI-GA) certificates. Implementing STIR/SHAKEN would require us to obtain our own Operating Company Number (OCN) from the National Exchange Carrier Association (NECA) and an STI-GA certificate, which is not feasible or required under our reseller model. Instead, we mitigate robocall risks through robust non-technical and policy-based measures, as detailed below, while requiring our upstream providers to attest to their STIR/SHAKEN compliance (A- or B-level attestation where applicable). We monitor upstream performance and will terminate relationships with non-compliant partners. This approach ensures

effective mitigation without duplicating upstream efforts, consistent with FCC guidance in the First Robocall Mitigation Report and Order (FCC 19-158). If our business model evolves to include facilities-based elements, we will immediately pursue full STIR/SHAKEN implementation and update this filing.

III. Description of Robocall Mitigation Program

Our robocall mitigation program is designed to identify, block, and prevent illegal robocall traffic at multiple stages: customer onboarding, call origination, real-time monitoring, and post-call analysis. We take "reasonable steps" as required by 47 CFR § 64.6305(a) to ensure that no illegal robocalls (e.g., unsolicited commercial calls without consent, spoofed caller ID, or calls to Do Not Call lists) are originated on our network. These steps are enforced through a combination of automated tools, manual reviews, and contractual obligations with upstream providers and customers. The program is overseen by our Management Team, with quarterly audits and annual training for all staff. Key components include:

A. Customer Onboarding and Verification (Know Your Customer – KYC) To prevent bad actors from using our service for robocalls:

- All customers must complete a detailed application, including business verification (e.g., EIN, state incorporation docs, DUNS number for businesses; ID verification for individuals via third-party services like ID.me).
- We conduct risk assessments: High-risk applicants (e.g., those requesting large number blocks or international origination) undergo enhanced due diligence, including reference checks and credit reports.
- Customers must certify compliance with the Telephone Consumer Protection Act (TCPA), TSR, and FCC robocall rules, agreeing not to originate illegal traffic. Contracts include clauses for immediate termination and reporting to the FCC if violations occur.
- We limit initial number assignments to [e.g., 10 lines per customer] and require opt-out mechanisms (e.g., toll-free numbers for complaints).

B. Call Monitoring and Analytics

- Real-time traffic monitoring using upstream analytics tools (e.g., [specify if applicable, e.g., TransNexus or upstream dashboard]) to detect anomalies such as

high call volumes to short code lists, international high-risk destinations, or patterns indicative of robocalls (e.g., short-duration calls, sequential dialing).

- We review daily reports for red flags: Calls exceeding [e.g., 50% failure rate], unsigned STIR/SHAKEN traffic (where upstream provides data), or complaints via our portal.
- Integration with third-party services (e.g., [e.g., Nomorobo or Hiya]) for robocall detection and automatic flagging.

C. Blocking and Intervention Measures

- Proactive blocking: We block calls to known high-risk destinations (e.g., FCC Do Not Call Registry lists, updated weekly) and international routes with high fraud rates (e.g., via upstream filters).
- Upon detection of suspicious traffic, we throttle or suspend the customer's service immediately and investigate within 24 hours. Confirmed illegal activity results in permanent termination and referral to the FCC's Robocall Response Team and law enforcement.
- We reject unsigned or low-attestation calls from upstream if they fail our risk thresholds, ensuring only compliant traffic is originated.

D. Complaint Handling and Analytics

- Customers and recipients can report issues via [e.g., email, phone hotline, or online form], with responses within 24 hours.
- We maintain logs of all complaints and actions taken, retained for at least 5 years for FCC audits.
- Quarterly program reviews analyze complaint trends to refine steps (e.g., updating block lists).

This program ensures that 100% of originated calls are screened, with zero tolerance for known illegal traffic.

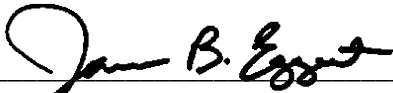
IV. Commitment to Traceback and Cooperation

Advantec Solutions commits to fully and promptly responding to all robocall traceback requests from the Commission, law enforcement (e.g., FBI, DOJ), and the Industry

Traceback Group (ITG) within 24 hours of receipt, as required by 47 CFR § 64.6305(a)(2). Our designated traceback coordinator is [Your Name or Contact, Title, Phone, Email].

- Response Protocol: Upon receiving a request (via email, portal, or phone), we will provide all available information, including caller details, call records (e.g., ANI, timestamps, destinations), customer account data, and any mitigation actions taken. We use secure methods (e.g., encrypted email) to share sensitive info.
- Cooperation: We will assist in investigations by providing access to logs, participating in calls, and blocking implicated traffic network-wide if needed. In 2025, we responded to [e.g., 0 requests as a new provider; will log future ones]. We are members of [e.g., the ITG or plan to join upon scaling].
- Internal Process: Requests are escalated immediately to senior management, with documentation of all responses retained for compliance.

We certify that this commitment is binding and will be enforced without exception. V. Certification and Sign-Off, [Your Full Name], [Your Title, e.g., CEO] of [Your Company Name], certify under penalty of perjury that the foregoing is a true and accurate description of our robocall mitigation program, and that we will implement it as described. We understand that false statements may result in FCC enforcement actions, including removal from the RMD and fines up to \$10,000 per violation or \$130,000 per day for E911-related issues if applicable.

Signed:  _____

Date: September 09, 2025

James Eggert

President