

Robocall Mitigation Plan

Smith Operating Solutions, LLC ("SOS")

Robocall Mitigation Database No. RMD0008543 | Filed: May 5, 2026

1. Principals, Affiliates, Subsidiaries, and Parent Companies

- **Designated Human Principal:** Adam Smith
- **Title:** Owner / Manager
- **Responsibility:** Mr. Smith is the primary individual responsible for the implementation and oversight of this Robocall Mitigation Plan, including customer vetting, call analytics monitoring, and regulatory compliance.
- **Affiliations:** SOS has no parent companies, subsidiaries, or affiliates at this time.

2. Disclosure of Past Enforcement Actions or Investigations

Pursuant to 47 CFR § 64.6305(d)(2)(iv) and the Commission's Robocall Mitigation Database ("RMD") filing instructions, Smith Operating Solutions, LLC ("SOS" or "the Company") provides the following description of the prior agency action to which it was subject. This description addresses each of the five elements required by the Commission's instructions and the WCB Frequently Asked Questions document released January 22, 2026.

(1) Law Enforcement or Regulatory Agencies Involved

The action was conducted entirely within the Federal Communications Commission (the "Commission" or "FCC"). Two FCC bureaus participated:

- **Wireline Competition Bureau ("WCB")** – administers the Robocall Mitigation Database, conducted the initial review of the Company's certification, and issued the original deficiency notification.
- **Enforcement Bureau ("EB")** – the deciding bureau, which issued the operative Show Cause Order and the Final Removal Order.

No other federal agency, state attorney general, the Industry Traceback Group ("ITG"), or other law enforcement body was involved. The matter was administered under FCC File No. EB-TCD-24-00036891, which was subsequently reassigned to File No. EB-TCD-25-00038590.

(2) Date the Action or Investigation Commenced

The matter commenced on March 29, 2024, when the WCB Robocall Mitigation Database team sent the Company an email notifying it that its RMD certification was noncompliant with 47 CFR § 64.6305 because the Company had not submitted an updated certification and updated robocall mitigation plan by the February 26, 2024 effective date established by the Commission's Sixth Caller ID Authentication

Order and Seventh Call Blocking Order. That notification directed the Company to cure the deficiency by April 29, 2024.

The matter then proceeded through the following stages:

- **December 10, 2024** – The Enforcement Bureau released its Show Cause Order (In the Matter of 2,411 Robocall Mitigation Database Filers, 39 FCC Rcd 13318), which named the Company among 2,411 providers and afforded a final opportunity to cure.
- **December 17, 2024** – Summary of the Show Cause Order published in the Federal Register (89 Fed. Reg. 102144), establishing a compliance deadline of December 31, 2024.
- **August 25, 2025** – The Enforcement Bureau adopted and released the Final Removal Order, FCC Order DA 25-737, which removed the Company's RMD certification (Database No. RMD0008543, listed in Appendix A to that Order).

(3) Current Status of the Action or Investigation

The Enforcement Bureau's Final Removal Order (DA 25-737) took effect upon release on August 25, 2025; removed the Company's certification from the RMD as of that date; and required all intermediate and voice service providers to cease accepting traffic directly from the Company within two business days of release.

On September 17, 2025, the Company received an email from the FCC's Robocall Mitigation Database team notifying the Company that its filing had been **provisionally reinstated** in the RMD, that downstream providers may resume accepting traffic from the Company under 47 CFR § 64.6305(g), and that the Company's downstream providers may be informed of the provisional reinstatement. The Bureau's notice expressly stated, however, that this *"provisional reinstatement is not a final determination regarding the compliance of the [C]ompany's filing with the Commission's rules"* and that "[d]eficiencies may still exist in [the] filing, which the [C]ompany should promptly address."

Accordingly, the current status of this matter is as follows: (a) the Company's RMD certification was removed by Final Order on August 25, 2025; (b) the Company was provisionally reinstated to the RMD on September 17, 2025, pending the Bureau's confirmation that all deficiencies in its filing have been cured; (c) the Company has, in response to subsequent communications from Commission staff, undertaken iterative corrections to its certification and to the mitigation plan attached to this filing; and (d) the present submission is intended to address all remaining deficiencies identified by Commission staff. The Company is not aware of any ongoing investigation, civil enforcement action, forfeiture proceeding, or referral arising from this matter, and no monetary forfeiture or other sanction beyond the August 25, 2025 removal has been imposed.

(4) Summary of the Findings of Wrongdoing

The Enforcement Bureau's findings, set forth in paragraphs 7 and 8 of DA 25-737, were limited to administrative deficiencies in the Company's RMD filing. Specifically, the Bureau found that the Company's RMD certification was deficient on two grounds:

- (a) the Company's robocall mitigation plan was either not provided or did not contain the information required to be submitted by the February 26, 2024 deadline established under 47 CFR § 64.6305; and
- (b) the Company's certification itself lacked information required by that same deadline.

The Bureau further found that, despite receiving the March 29, 2024 deficiency notification from WCB and the December 10, 2024 Show Cause Order from the Enforcement Bureau, the Company failed either to cure the deficiency or to file a response explaining why its certification should not be removed.

Importantly, the Bureau did not find that the Company originated, transmitted, encouraged, assisted, or otherwise facilitated illegal robocalls or unlawful spoofing. The wrongdoing identified was the inadequacy of the Company's prior RMD certification and mitigation program description, not any underlying illegal calling activity. The Company's name does not appear in the August 6, 2025 Initial Removal Order (DA 25-694), which separately identified 185 providers that had additionally been associated with suspected illegal robocall traffic and traceback non-responsiveness.

(5) Whether Any Final Determinations Have Been Issued

Yes. A final determination was issued in the form of FCC Order DA 25-737, adopted and released August 25, 2025, by the Acting Chief of the Enforcement Bureau pursuant to the authority delegated under 47 CFR §§ 0.111 and 0.311. That Order:

- found the Company's RMD certification deficient;
- removed the certification from the RMD effective upon release;
- directed all intermediate and voice service providers to cease accepting traffic directly from the Company within two business days; and
- prohibited the Company from refiling in the RMD absent the prior consent of both the Wireline Competition Bureau and the Enforcement Bureau.

No monetary forfeiture, civil penalty, consent decree, or other sanction beyond removal was imposed, and no finding of intentional wrongdoing was made. The Bureau's subsequent September 17, 2025 provisional reinstatement of the Company to the RMD is, by its own terms, expressly not a final determination regarding the compliance of the Company's filing. No other final determination, by the FCC or any other agency, has been issued against the Company in connection with this matter.

Remediation and Resolution

In response to the findings in DA 25-737, the Company has conducted a comprehensive review of its prior submission and has prepared the updated, fully detailed robocall mitigation plan set forth in this document to address each category of information required by 47 CFR § 64.6305(d)(2). The Company is submitting this revised plan and certification pursuant to the consent process contemplated by paragraph 13 of DA 25-737 and to ensure full, ongoing compliance with the Commission's rules.

3. Detailed Know Your Customer (KYC) Plan

SOS employs a multi-layered verification process to prevent illegal robocallers from gaining access to its Hosted PBX platform:

- **Identity & Business Verification:** SOS collects and verifies the applicant's Employer Identification Number (EIN) or Tax ID and business registration documents to ensure the entity is a legally recognized business.
- **Mandatory Live Authentication:** SOS severely limits the capabilities of new accounts until the customer completes a live phone call with a support representative to confirm the identity of the individual and the company they represent.
- **Use-Case Vetting:** SOS screens all applicants to determine if they intend to use services for autodialing from a database for telemarketing.
- **Consent Requirements:** SOS requires that any telemarketing traffic have written permission from the called parties.
- **Restricted Access:** New accounts remain in a restricted state with limited capabilities until the verification process, including the live call, is successfully completed.

4. Traceback Compliance and Cooperation

Pursuant to 47 CFR § 64.6305(a)(2), SOS commits to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use SOS's service to originate calls. All voice traffic originated by SOS's customers through its Hosted PBX platform is subject to this robocall mitigation program.

5. Call Pattern Monitoring and Analytics System

SOS operates a hosted private branch exchange ("Hosted PBX") platform built on VitalPBX, on which SOS's end-user customers and their endpoints are provisioned. Customer call traffic is routed through the Hosted PBX platform and then handed off to SOS's upstream voice service provider (Telnyx LLC) for delivery to the public switched telephone network. SOS has full operational control over its Hosted PBX platform, including the ability to apply call routing logic, blocking rules, rate limits, and account-level restrictions to customer traffic at that layer.

SOS uses VitalPBX Sonata Stats to continuously monitor calling patterns on the Hosted PBX platform and to identify fraudulent traffic, including robocalling, traffic pumping, and international toll fraud. The system flags:

- High-volume short-duration calls
- Spikes in call attempts to unassigned or invalid numbers
- Sudden changes in call destinations
- Unusual calling patterns deviating from normal traffic flows

Traffic flagged by these systems is reviewed by compliance staff. Where illegal or fraudulent activity is confirmed, SOS blocks the offending traffic at the Hosted PBX layer and, where warranted, suspends or terminates the customer account responsible for the traffic, consistent with Section 6 of this Plan.

6. Contractual Compliance and Enforcement

- **Service Agreements:** SOS requires by contract that all users of its services comply with applicable laws prohibiting illegal robocalling.
- **Termination:** SOS provides for the immediate blocking or termination of services for any customer found to be in breach of these provisions or engaged in intentional violations.
- **Upstream Provider Requirements:** SOS routes its outbound customer traffic exclusively through upstream voice service providers that are listed in the FCC's Robocall Mitigation Database. To the extent SOS in the future accepts inbound off-network traffic for termination, SOS will accept such traffic only from third-party carriers listed in the RMD, consistent with 47 CFR § 64.6305(g).
- **Know-Your-Upstream-Provider Procedures:** Pursuant to 47 CFR § 64.6305(d)(2)(ii)(C), SOS uses Telnyx LLC as its principal upstream provider for PSTN termination of customer calls. Telnyx is a duly registered voice service provider listed in the Robocall Mitigation Database and has implemented STIR/SHAKEN call authentication on its IP network. SOS verifies, on an ongoing basis, that any upstream provider through which its customer traffic is delivered to the PSTN remains in good standing in the RMD before continuing to route traffic through that provider. SOS will discontinue use of any upstream provider that is removed from the RMD or that becomes the subject of an enforcement action related to illegal robocalling.

7. STIR/SHAKEN Implementation Status

The Company has not implemented STIR/SHAKEN call authentication and does not claim a categorical extension under 47 CFR § 64.6304. Pursuant to the alternative provision in 47 CFR § 64.6305(d)(2)(i), the Company is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN — specifically, the IP-PSTN gateway and signing infrastructure at which STIR/SHAKEN authentication is technically performed. The Company's lack of control is limited to that signing layer; the Company exercises full operational control over its Hosted PBX platform, where its robocall mitigation program (described in Sections 3 through 6 and 8 of this Plan) is implemented and enforced.

The Company is a voice service provider that delivers calls originated by its end-user customers to the public switched telephone network through Telnyx LLC, an upstream voice service provider. The IP network facilities at which STIR/SHAKEN authentication is technically performed — including the session border controllers, signing infrastructure, and the originating provider's STI-CA certificate — are owned and operated by Telnyx, not by the Company. The Company does not hold, and under current Secure Telephone Identity Governance Authority ("STI-GA") policy is not currently positioned to obtain, an Operating Company Number (OCN), an SPC token issued by the STI Policy Administrator (iconectiv), or a STIR/SHAKEN certificate issued by an STI Certification Authority. Accordingly, the Company has no

technical means to authenticate calls under its own certificate on the infrastructure through which its customer traffic is delivered.

This position is consistent with the Commission's longstanding determination that providers that lack control over the facilities necessary to implement STIR/SHAKEN do not have an implementation obligation. See First Caller ID Authentication Report and Order, 35 FCC Rcd 3241, 3260, para. 40 (2020); Wireline Competition Bureau, Triennial Report on the Efficacy of the Technologies Used to Implement Caller ID Authentication Information, n.27 (Dec. 2022). It is further consistent with the framework articulated in the Commission's Eighth Report and Order (FCC 24-119, adopted Nov. 2024), under which the STIR/SHAKEN implementation obligation attaches to the provider with control over the network infrastructure where authentication occurs.

Voice traffic originated by the Company's end-user customers is independently authenticated at the Telnyx layer. Telnyx is itself a voice service provider duly registered in the Robocall Mitigation Database, and Telnyx applies STIR/SHAKEN authentication under its own certificate and OCN to traffic originating on the Telnyx platform. The Company does not represent that this upstream authentication constitutes STIR/SHAKEN implementation by the Company for purposes of 47 CFR § 64.6305, and the Company has not entered into any third-party authentication arrangement of the kind contemplated by the Eighth Report and Order under which the Company would be the provider with the implementation obligation.

In lieu of STIR/SHAKEN implementation, the Company has implemented and continues to maintain the comprehensive robocall mitigation program described in Sections 3 through 9 of this Plan, which fully satisfies the Company's obligations under 47 CFR § 64.6305(a). Should the Company in the future obtain the credentials and network control necessary to authenticate calls under its own STIR/SHAKEN certificate, the Company will update its RMD certification to reflect the change within 10 business days, consistent with 47 CFR § 64.6305(d)(5).

8. Internal Compliance and Escalation

SOS is a single-principal operation in which Adam Smith, as Owner / Manager, serves as the designated individual responsible for all robocall mitigation and traceback compliance functions. SOS's internal protocols include the following:

- **Ongoing Training and Awareness:** The designated principal maintains current knowledge of robocall mitigation requirements through review of FCC orders and Public Notices, the Wireline Competition Bureau's Robocall Mitigation Database guidance and Frequently Asked Questions, STI-GA policy updates, and industry traceback consortium communications.
- **Escalation Path:** Suspicious traffic flagged by the analytics systems described in Section 5, and complaints received from traceback entities, downstream carriers, or consumers, are reviewed promptly by the designated principal, who has direct authority to block traffic at the Hosted PBX layer and to suspend or terminate customer accounts under the contractual provisions described in Section 6.
- **Complaint Handling:** SOS reviews and remediates complaints from traceback entities, carriers, and consumers on an immediate basis, consistent with its 24-hour traceback response commitment under 47 CFR § 64.6305(a)(2).

9. Filing Updates and Security

SOS will update all information in the Robocall Mitigation Database within 10 business days of any change, consistent with 47 CFR § 64.6305(d)(5). SOS will complete annual recertification filings on or before March 1 each year. SOS enforces secure access protocols for database submissions, including multi-factor authentication.

Adam Smith

Owner / Manager

Smith Operating Solutions, LLC

Date: May 5, 2026