

Robocall Mitigation Plan

**SPARK I/T Services LLC 105 North York Street, Muskogee, OK 74403 Effective Date:
February 25, 2026**

I. Introduction

This Robocall Mitigation Plan (the "Plan") is submitted by SPARK I/T Services LLC (the "Company") pursuant to the requirements of 47 C.F.R. § 64.6305, as established by the Federal Communications Commission (FCC). The Company provides secure and reliable Voice over Internet Protocol (VoIP) services through its hosted 3CX platform and is committed to combating the proliferation of illegal robocalls. This Plan details the affirmative, effective measures the Company has taken to prevent the origination of illegal robocall traffic on its network.

This Plan describes the specific, reasonable steps the Company has taken to avoid originating illegal robocall traffic, including its Know Your Customer (KYC) procedures, its reliance on a compliant upstream provider, its use of platform-specific mitigation tools, and its commitment to cooperate fully with traceback requests from the FCC, law enforcement, and the industry traceback consortium. This Plan is filed in conjunction with the Company's certification in the FCC's Robocall Mitigation Database (RMD).

II. STIR/SHAKEN Implementation Status

As required by 47 C.F.R. § 64.6305, the Company certifies its STIR/SHAKEN implementation status in the FCC's Robocall Mitigation Database. The Company's current status is as follows:

No Implementation: The Company has not implemented the STIR/SHAKEN authentication framework on its own network. As a provider utilizing a hosted platform, the Company relies on its underlying carrier, Bandwidth.com, which is fully compliant with the STIR/SHAKEN framework, to perform call authentication. The Company has an extension pursuant to 47 C.F.R. § 64.6304 due to a lack of direct control over the network infrastructure necessary to implement STIR/SHAKEN. All calls originated by the Company's customers are subject to the mitigation measures described in this Plan.

III. Robocall Mitigation Program

The Company has implemented a multi-layered robocall mitigation program that includes the following components. The Company certifies that it complies with the practices described herein and that it does not knowingly or through negligence originate illegal robocall traffic.

A. Commitment to Traceback Cooperation

The Company commits to responding fully and within 24 hours to all traceback requests received from the FCC, law enforcement, and the industry traceback consortium (the Industry Traceback Group, or ITG). The Company will cooperate with these entities in investigating and stopping any illegal robocallers that use its service. The Company's designated robocall mitigation point of contact is identified in Section V of this Plan.

B. Know Your Customer (KYC) Procedures

In accordance with 47 C.F.R. § 64.1200(n)(4), the Company has established affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls. The Company's KYC procedures include:

- **Customer Onboarding Verification:** Prior to activating service, the Company conducts due diligence on all clients to verify their identity and the legitimacy of their intended use of our services. This includes collecting and verifying business information, physical address, and contact details to ensure adherence to legal and ethical communication practices.
- **Contractual Prohibitions:** The Company's service agreements and acceptable use policies explicitly prohibit customers from using the Company's services to originate illegal robocalls or engage in fraudulent or deceptive activities. These agreements grant the Company the right to suspend or terminate service for any violation of these terms.

C. Know Your Upstream Provider Procedures

The Company utilizes Bandwidth.com as its underlying VoIP carrier. The Company verifies that Bandwidth.com has an active, compliant filing in the FCC's Robocall Mitigation Database and is in good standing. The Company will not use an underlying carrier that is not listed in the RMD.

D. Call Traffic Monitoring and Mitigation Tools

The Company leverages the capabilities of its hosted 3CX platform to monitor and mitigate suspicious activities indicative of illegal robocalls. This proactive approach enables us to address potential issues promptly. Specific measures include:

- **Digital Receptionist (IVR) Configuration:** We utilize 3CX's Digital Receptionist to screen incoming calls. Callers may be prompted to interact (e.g., "Press 1 to connect"), a method effective in filtering out automated robocalls that cannot respond to such prompts.
- **Call Flow Designer (CFD) Utilization:** For advanced call handling, we employ 3CX's Call Flow Designer to create custom call flows that can identify and manage suspicious call patterns, enhancing our ability to mitigate potential robocalls.
- **Blacklist Management:** We maintain and regularly update a blacklist of known spam numbers within the 3CX management console. Additionally, the 3CX platform maintains a global blacklist of IP addresses associated with malicious activities, which are automatically blocked to enhance security.
- **Traffic Analysis:** Our systems continuously monitor call patterns to detect anomalies such as unusually high call volumes, high volumes of short-duration calls, or other patterns that may indicate illegal robocalling.

E. Employee Training

The Company educates its team on recognizing and appropriately handling potential robocalls and suspicious customer activity to prevent engagement with or facilitation of fraudulent activities.

F. Commitment to Continuous Improvement

The Company is dedicated to regularly reviewing and enhancing our robocall mitigation strategies to adapt to emerging threats, evolving technologies, and new regulatory requirements to maintain the highest standards of service integrity.

IV. Prior Regulatory Actions

In the past two years, neither SPARK I/T Services LLC nor any entity with which the Company shares common ownership, management, directors, or control has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the transmitting, encouraging, assisting, or otherwise facilitating of illegal robocalls or spoofing.

V. Robocall Mitigation Point of Contact

All traceback requests and inquiries related to robocall mitigation should be directed to the following designated point of contact:

Field	Information
Name	[Insert Contact Name]
Title	[Insert Title]
Company	SPARK I/T Services LLC
Business Address	105 North York Street, Muskogee, OK 74403
Telephone Number	(918) 608-8888
Email Address	[Insert Email Address]

VI. Certification

I, the undersigned, am an officer of SPARK I/T Services LLC and am authorized to make this certification on behalf of the Company. I certify, under penalty of perjury pursuant to 47 C.F.R. § 1.16, that all statements made in this Robocall Mitigation Plan are true, complete, and correct to the best of my knowledge and belief, and are made in good faith.

Field	Information
Signature	_____
Printed Name	[Name]
Title	[Title]
Company	SPARK I/T Services LLC
Date	[Date]

VII. Regulatory References

[1] 47 C.F.R. § 64.6305 — Robocall mitigation and certification. [2] 47 C.F.R. § 64.1200(n)(4) — Know Your Customer obligations. [3] FCC Robocall Mitigation Database — <https://fccprod.servicenowservices.com/rmd>