



Door Access | Video Surveillance | Data Cabling
VoIP/Hosted Phone Systems | Fiber Optics | Paging

Robocall Mitigation Program Plan for SCI Communications

This Robocall Mitigation Program (RMP) Plan outlines the measures SCI Communications will implement to prevent the origination and transmission of illegal robocalls on its network, in compliance with the Federal Communications Commission (FCC) regulations, including those stemming from the TRACED Act. This plan is designed to be detailed, actionable, and subject to ongoing review and improvement to ensure its effectiveness in significantly reducing illegal robocall traffic.

1. Introduction and Commitment

SCI Communications is committed to combating illegal and unwanted robocalls and maintaining the integrity of the public switched telephone network (PSTN). This RMP details the specific reasonable steps SCI Communications will take to prevent unlawful robocalls from originating on its network and to cooperate with traceback efforts. This plan is submitted in accordance with FCC requirements for voice service providers that have not fully implemented STIR/SHAKEN or are operating under an extension.

2. STIR/SHAKEN Implementation Status

SCI Communications acknowledges the FCC's mandate for STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted information using Tokens) implementation. As of 2025-09-04, SCI Communications has **partially implemented the STIR/SHAKEN authentication framework in the IP portions of its network**. This partial implementation means that while some calls originating on our network are signed with STIR/SHAKEN attestations, a comprehensive, end-to-end deployment across all IP-based voice traffic is still in progress. We are actively working towards full deployment and will update our certification in the Robocall Mitigation Database (RMDb) as our implementation progresses.

3. Robocall Mitigation Program Details

SCI Communications' Robocall Mitigation Program encompasses a multi-faceted approach to identify, prevent, and mitigate illegal robocall traffic. Our program includes the following key elements:

- **Network Monitoring and Analytics:**
 - SCI Communications will deploy and utilize **advanced call analytics systems to identify and block illegal traffic originating from or**

SCI – 2001 East Army Post Road suite C Des Moines, Iowa 50320
515-339-7860 Phone / 515-381-3906 Fax
www.sci-iowa.com



Door Access | Video Surveillance | Data Cabling
VoIP/Hosted Phone Systems | Fiber Optics | Paging

transiting its network. This includes monitoring call patterns, call volumes, call duration, answer-seizure ratios (ASR), and other anomalous behaviors indicative of illegal robocalling campaigns.

- We will leverage a combination of in-house tools and third-party vendor solutions for real-time traffic analysis. (Specific vendor names will be provided in a confidential attachment, if applicable, to protect proprietary information).
- Regular audits of network traffic will be conducted to identify potential sources of illegal robocalls and to assess the effectiveness of our mitigation efforts.
- **Know Your Customer (KYC) Policy and Due Diligence.**
 - SCI Communications will implement and enforce a **robust Know Your Customer (KYC) policy for all new and existing customers** that originate voice traffic on our network. This policy will include:
 - Verification of customer identity and business legitimacy.
 - Assessment of the customer's intended use of voice services.
 - Collection of accurate contact information for all customers, including principals and points of contact responsible for robocall mitigation.
 - Ongoing monitoring of customer activity to detect changes in traffic patterns that may indicate a shift towards illegal robocalling.
 - Contractual terms with customers will explicitly prohibit the origination of illegal robocalls and include provisions for immediate service termination upon violation.
- **Traffic Management and Blocking:**
 - SCI Communications will **actively block calls identified as illegal robocalls based on network analytics, traceback requests, and credible reports of illegal activity.** This blocking will be implemented in a manner consistent with FCC rules, ensuring that legitimate calls are not inadvertently blocked.
 - We will establish and maintain internal thresholds and criteria for identifying and blocking suspected illegal traffic.
 - In cases where a customer is identified as originating illegal robocalls, SCI Communications will take swift action, which may include:
 - Issuing warnings and requiring corrective action.
 - Implementing call volume restrictions or rate limits.
 - Suspending or terminating service, in accordance with contractual agreements and FCC regulations.



Door Access | Video Surveillance | Data Cabling
VoIP/Hosted Phone Systems | Fiber Optics | Paging

- **Response to Traceback Requests and Cooperation with Authorities:**
 - SCI Communications commits to **responding within 24 hours to all traceback requests from the FCC, law enforcement agencies, and the Industry Traceback Consortium (ITC)**. This includes providing all requested information to assist in identifying and stopping illegal robocallers.
 - We will cooperate fully with investigations conducted by the FCC, law enforcement, and the ITC into illegal robocalling activities originating from or transiting our network.
 - Our designated point of contact for robocall mitigation-related issues is:
 - Jerry Brown
 - Vice President
 - Owner
 - 2001 E Army Post Road Suite C Des Moines, Iowa 50320
 - 515-339-7860
 - jerry@sci-iowa.com
- **Employee Training and Awareness:**
 - SCI Communications will provide **regular training to relevant personnel** on robocall mitigation policies, procedures, and the importance of compliance with FCC regulations.
 - Employees will be educated on identifying suspicious traffic patterns and reporting potential illegal robocalling activities.
- **Continuous Improvement:**
 - This RMP will be **periodically reviewed and updated** to reflect changes in FCC regulations, industry best practices, and the evolving tactics of illegal robocallers.
 - SCI Communications will actively participate in industry forums and collaborate with other voice service providers to share information and strategies for combating robocalls.
-

4. Attestation and Compliance

SCI Communications understands that the STIR/SHAKEN standards are designed to convey the validity and origin of a number, not necessarily the legality of a call itself. Therefore, our RMP goes beyond mere attestation levels (A, B, or C) and focuses on actively reducing the origination of illegal or bad traffic from our network. We will assign attestation levels based on our knowledge of the traffic on our network, as per STIR/SHAKEN standards.

SCI – 2001 East Army Post Road suite C Des Moines, Iowa 50320
515-339-7860 Phone / 515-381-3906 Fax
www.sci-iowa.com



Door Access | Video Surveillance | Data Cabling
VoIP/Hosted Phone Systems | Fiber Optics | Paging

SCI Communications acknowledges that failure to adhere to this RMP or to conduct necessary due diligence to prevent the origination of bad traffic could lead to enforcement action by the FCC, including potential removal from the Robocall Mitigation Database and prohibition from accepting traffic from other providers.

5. Certification and Updates

SCI Communications certifies that the information provided in this Robocall Mitigation Program Plan is true and correct to the best of its knowledge and belief. We understand that we are required to update this submission within 10 business days of any changes to the required content.

This plan will be uploaded as a PDF file to the FCC's Robocall Mitigation Database via the portal at <https://www.fcc.gov/robocall-mitigation-database>.

6. Extension Category (if applicable)

SCI Communications qualifies for the small voice service provider extension, as it has 100,000 or fewer subscriber lines. We are certified to this extension category.

7. Accountability Measures

SCI Communications understands the importance of accurate and up-to-date information in the Robocall Mitigation Database. We acknowledge the FCC's ongoing efforts to improve the quality of submissions and increase accountability. We will comply with all requirements regarding the accuracy of our CORES registration information, multi-factor authentication for RMDB access, and any future requirements for obtaining a unique Personal Identification Number (PIN) for submissions, as proposed by the FCC. We also understand the potential for forfeiture amounts for submitting inaccurate or false information or failing to update information within the required timeframe.