



**Sagecom Incorporated**

**FRN - 0022924518**

**Robocall Mitigation Plan**

**RMD File Number - RMD0007295**

**Updated Date - December 23, 2024**

SageCom Inc. submits this Robocall Mitigation Plan ("Plan") pursuant to 47 C.F.R. § 64.6305 on behalf of itself. SageCom provides Unified Communications as a Service ("UCaaS") to individuals and business customers. This Plan describes SageCom's efforts to mitigate illegal robocalls consistent with the FCC's rules. SageCom may modify, add, delete, or otherwise alter any part of this Plan to respond to changes in its business, technologies, needs, industry best practices, or any applicable law or regulations.

The Robocall Mitigation Plan sets forth the actions SageCom takes to:

- I. SCREEN its customers before providing voice services ("Know-Your-Customer");
- II. MONITOR existing customers for traffic patterns and other information indicative of either having the potential to transmit fraudulent robocalls or transmitting the same and
- III. MITIGATE the transport of fraudulent robocall traffic via SageCom.

---

## I. SCREEN

SageCom undertakes the following Know-Your-Customer ("KYC") activities before providing voice services to end-users:

- A. **Information Collection.** All SageCom customers must provide their names, addresses, verifiable e-mail address(es), verifiable phone number(s), and validated payment information.
- B. **Information Validation.** New and renewing users must provide and maintain accurate and complete information about themselves to SageCom. Sagecom services Use Policy requires:
  1. All account and registration information, including the customer's legal name and contact information, is accurate, legal, legally obtained, and complete,
  2. Promptly update such information as needed to ensure its accuracy, and
  3. Promptly verify such information during service registration. SageCom uses third-party verification tools to validate information potential customers and customers provide. In addition, Sagecom monitors the IP addresses initiating orders, credit card payments, and device log-ins to identify and address anomalous behavior on customer accounts
- C. **Contractual Provisions.** Customers must agree to SageCom's terms of service that prohibit fraudulent traffic. Additionally, the terms of service state that SageCom may suspend or terminate services for violating SageCom's acceptable use provisions. Customers may also be held liable for any financial penalties imposed on SageCom for fraudulent traffic sent from the customer. The Use Policy can be found at: <https://www.sagecominc.com/product-and-service-terms/>
- D. **Know Your Upstream Provider.**
  1. **Procurement Processes.** SageCom has a robust procurement process that includes sanctions screening and collecting documentation and information about its upstream providers that includes, but is not limited to:
    - a. Contact Person(s);
    - b. State or country of incorporation; and,
    - c. Federal tax identification number and FCC Registration ID
    - d. Network Details such as IP Address and Network connectivity configuration
  2. **Contractual Terms.** SageCom's contracts with upstream providers require that the provider comply with all relevant laws, including, in many instances, specific provisions prohibiting the transmission of fraudulent traffic and robocalls. SageCom's contracts also permit SageCom to terminate the upstream provider's right to send traffic to SageCom if any contractual provision is violated.

## II. MONITOR.

A. **Traffic Patterns.** SageCom continuously monitors its customers' traffic patterns for indicators of fraudulent calls, such as:

1. Short-duration calls less than 6 seconds long;
2. Multiple calls per minute from the same customer.
3. Low call answer rates for calls from a particular customer.
4. Calls to high fraud destinations.
5. Dialing patterns.
6. Calls to numbers on Do-Not-Call lists.
7. Traceback requests; and
8. Unusual changes in a customer's established traffic patterns.

B. **SPAM Labeling.** As a voice service provider serving end-users, Sagecom fully implemented the STIR/SHAKEN Caller ID Authentication Framework across its network as of June 23, 2021. SageCom uses a third-party vendor, Bulk Solutions, to monitor its domestic call origination and termination for likely fraud. Customers will receive a "spam" indicator prepended to their CNAM display if they receive a call from a suspected robocaller. The spam indicator is based on a proprietary combination of indicators assembled by Bulk Solution.

## III. MITIGATE

A. **Commitment to Respond to Traceback Requests.** SageCom commits to responding fully and within twenty-four (24) hours to traceback requests from law enforcement, the Federal Communications Commission, and the industry traceback consortium and to cooperating with such entities to investigate and stop illegal robocalls that use its services.

B. **Robocall Mitigation Database Filings.** SageCom checks the Robocall Mitigation Database and only accepts calls from the following categories of providers if those providers' filings appear in the Robocall Mitigation Database and that filing has not been delisted according to enforcement action:

1. Domestic voice service providers.
2. Foreign voice service providers or foreign intermediate providers that use North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States; and,
3. Gateway providers.

C. **Blocking/Discontinuance.** SageCom employs various effective measures to block fraudulent calls. When SageCom identifies fraudulent traffic or traffic with a high likelihood of being fraudulent, it will take prompt action to block such traffic. In addition to blocking the offending traffic, SageCom may suspend or terminate the offending customer's service.

D. **Selective Call Blocking.** Certain SageCom products have selective call blocking that rejects or sends incoming calls to voicemail based on their risk profile, which is determined by the Geo Risk validation status and Telephone Number (TN) validation.

---

This Robocall Mitigation Plan describes the specific measures that SageCom implemented as of December 30, 2024. SageCom continually evaluates the efficacy of its measures to combat bad actors and takes appropriate steps to improve these measures when needed.