

Robocall Mitigation Plan (2024)

Company Name: SIPspace

Company Address: 415 Antique City Dr Ste 1, Walnut, IA

Company Phone: (844) 576-2555

This Robocall Mitigation Plan is submitted by ThinkspaceIT d/b/a SIPspace Communications pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC), which require all “voice service providers” to establish a “robocall mitigation plan.” This document sets forth the SIPSpace’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network.

SIPSpace views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network. In addition to following these steps, SIPSpace commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and cooperating with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

I. STIR/SHAKEN Implementation Status

SIPspace offers full STIR/SHAKEN compliance to all clients and incorporates it into all new accounts and hardware upgrades. Legacy clients with equipment that does not currently support STIR/SHAKEN are encouraged to upgrade, with recommended timelines and migration plans designed to achieve full compliance.

To mitigate potential risks from legacy systems, SIPspace employs alternative measures, such as rigorous monitoring and enhanced traceback cooperation, until full STIR/SHAKEN adoption is achieved across its network.

SIPspace has established methods and procedures to monitor its network and detect and prevent fraudulent activity. The company uses call authentication, call labeling, and call blocking services to protect its networks and consumers from harmful calls. SIPspace also deploys software to monitor daily network usage and has methods in place to address issues as soon as they are identified.

SIPspace fully complies with all conditions set forth in the FCC’s 47 C.F.R. § 64.6301.

II. Traceback Requests

SIPspace will cooperate with the FCC, law enforcement, and the Industry Traceback Group (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, SIPSpace dedicates sufficient resources to promptly complete and provide responses to all traceback requests. SIPspace commits to responding to any traceback request received within 24 hours.

A Network Security Specialist has been designated as the point of contact for addressing traceback requests. SIPspace has provided the ITG with the contact information and business hours for this individual or will do so upon receipt of the first request from the ITG. The point of contact ensures prompt, accurate, and comprehensive responses to all traceback requests.

III. Customer Vetting Practices

SIPspace employs robust Know Your Customer (KYC) practices to prevent or minimize the origination of illegal robocalls through its voice services. These practices apply to all voice service subscribers, including residential and business/commercial clients.

Vetting Process:

- Collect and verify customer information, including physical address, contact persons, state or country of incorporation, federal tax ID, and the nature of the customer's business.
- Require customers to execute service agreements that explicitly prohibit illegal robocalling and outline penalties for non-compliance.
- For high-risk customers (e.g., those with complex service configurations or high call volumes), conduct additional reviews such as background checks and site visits.

SIPspace also evaluates the intended usage of telephone number resources during the provisioning process to ensure legitimate activity. Customers demonstrating unusual or inconsistent usage patterns are flagged for further investigation.

IV. Ongoing Robocall Mitigation Practices

SIPspace monitors network usage and call detail records (CDRs) regularly to detect suspicious call activity or patterns indicative of illegal robocalls.

Key Indicators of Suspicious Activity:

1. Higher-than-normal subscriber traffic volumes, including large bursts of traffic in short timeframes.
2. Originating calls with short durations and low completion percentages.
3. Sequential dialing patterns.
4. Calls to invalid numbers.
5. Calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

When irregularities are detected, SIPspace investigates promptly to identify the party responsible. Actions taken may include customer notifications, service suspension, or termination.