

**Business Information**

Solutionreach Inc.
2600 N. Ashton Blvd.
Lehi, UT 84043

Contact Information

Thomas Skinner
General Counsel
legal@solutionreach.com

Solutionreach, Inc. Robocall Mitigation Plan

The FCC requires all voice service providers (“VSPs”) to certify in the Robocall Mitigation Database (“RMD”) that they have implemented a Robocall Mitigation Plan (“RMP”) to ensure that they do not originate illegal robocalls, pursuant to 47 CFR § 64.6305 (d).

VSPs are required to develop and implement a RMP that includes the following:

- reasonable steps the VSP is taking to avoid originating illegal robocall traffic
- a commitment by the VSP to respond within 24 hours to traceback requests from the Commission, law enforcement, and the industry traceback consortium (the “Traceback Entities”)
- a commitment by the VSP to cooperate with the Traceback Entities in investigating and stopping illegal robocallers from using its service to originate calls
- certification by the VSP that all calls originated by it are subject to a RMP and that no prior certifications have been removed by Commission action and that it has not been prohibited from filing in the RMD
- certification by the VSP that it has fully implemented the STIR/SHAKEN authentication framework across its entire network and that all calls are compliant with § 64.6301(a)(1) and (2)
- the specific reasonable steps taken by the VSP to avoid originating illegal robocall traffic, including how it complies with the obligation to know its customers, procedures to know its upstream providers, and the analytics systems it uses to identify and block illegal traffic (including the names of vendors if using third-party analytics)
- a statement of whether, at any time in the prior two years, the VSP has been subject to a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing related to facilitating illegal robocalls or spoofing, or a deficient RMD certification or RMP

The FCC states that a RMP developed by a VSP is sufficient if the practices described in it can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Overview

Solutionreach, Inc. (“Solutionreach”) is a very small VSP committed to complying with all applicable federal regulations, including those aimed at mitigating illegal robocalls. As a patient relationship management software provider, we understand the importance of maintaining the trust and security of communications between our customers (healthcare providers) and their patients. To that end, this document outlines Solutionreach’s comprehensive RMP, detailing the specific steps we have taken to prevent the origination, transmission, and termination of illegal robocalls.

As described herein, we utilize reputable telecommunications carriers for our voice traffic. These carriers have implemented robust robocall mitigation strategies, including STIR/SHAKEN technology, to ensure the integrity of calls placed through our services over their networks.

Robocall Mitigation

Solutionreach has implemented a RMP covering calls initiated using its services. This program includes the following key elements:

Know Your Customer: A Solutionreach customer is a healthcare provider entity that has a business relationship with Solutionreach, and for whom our services are used to transmit, originate, and/or terminate calls. Solutionreach verifies the business activity and identity of every customer during the contracting process, throughout onboarding, and at renewal. Verification data collected includes, but is not limited to: name, email address, physical address, credit card information, federal employer identification number (“EIN”), and national provider identification number (“NPI”).

Customers are required to update their information on subsequent orders and renewals. Customers are also required to further verify themselves when contacting Solutionreach for assistance. These verification procedures help to prevent fraudulent activity and ensure that our services are not used for illegal or unethical purposes.

In addition, Solutionreach requires every customer to register with The Campaign Registry in order to be able to send text messages using its services. Although this is not within the scope of voice calls, it is an added layer of verification, which further ensures proper identification of the customer.

The accurate identification of a customer in the STIR/SHAKEN ecosystem, discussed below, is tied to a telephone number-based caller identity associated with that customer.

Acceptable Use: Solutionreach requires customers to adhere to Acceptable Use Restrictions before being permitted to use Solutionreach's services. Among other things, such restrictions prohibit:

- creating a false identity or otherwise attempting to mislead any person as to the identity, source or origin of any message or phone call
- transmitting any unsolicited communications
- engaging in any conduct that is not in compliance with the consumer protection requirements of the Telephone Consumer Protection Act ("TCPA")
- engaging in any act that violates any other applicable law or regulation

Solutionreach may suspend or terminate services for violation of contractual terms, including its Acceptable Use Restrictions.

Limited Scope: Solutionreach's voice services are intentionally architected and designed to be limited in scope to prevent robocall abuse by customers as follows:

- calls are initiated only when required by a customer's system of record for patients (based on a patient's scheduled/due appointment or similar healthcare need)
- phone numbers cannot be randomly generated or dialed
- phone numbers cannot be sequentially dialed

Know-Your-Upstream-Provider: Solutionreach exercises reasonable due diligence with respect to its immediate upstream voice traffic providers. We have contractual relationships with a select group of carriers to originate and terminate voice and messaging traffic and these providers are chosen in part based on their strong commitment to robocall mitigation and adherence to industry best practices, including full implementation of STIR/SHAKEN call authentication technology.

Our current providers include:

- Broadband Dynamics, L.L.C. (FRN: 0006833412)
- Vonage Holdings Inc. (FRN: 0018401844)
- Bandwidth.com CLEC, LLC (FRN: 0017042060)

Each of these providers is certified in the RMD, demonstrating their compliance with FCC regulations and assuring readily accessible contact information for robocall mitigation-related inquiries. We maintain close communication with these upstream providers to ensure ongoing adherence to evolving robocall mitigation standards and to ensure we can appropriately contact them in the event we identify instances of suspicious activity.

Call Monitoring and Analytics: Solutionreach receives data and reports from upstream carriers from time to time. The data consists of reports on call volume, duration, and other key metrics. This data is not routinely analyzed to identify any irregular activity, such as sudden

spikes in call volume or calls from suspicious sources. Internal systems are regularly monitored for unusual and suspicious activity.

STIR/SHAKEN Implementation: Solutionreach has worked with its upstream voice traffic providers to ensure its protocols and procedures comply with the STIR/SHAKEN framework, to the extent we control those aspects. We rely on the implementation of our upstream providers to further fulfill the requirements of the STIR/SHAKEN standards.

We maintain close partnerships with our upstream providers, formalized through contracts that outline our shared commitment to compliance with industry best practices. We are intimately familiar with their services and regularly communicate with them on a variety of matters, including adherence to evolving FCC regulations.

Traceback Cooperation and Blocking: Solutionreach is committed to fully cooperating with all Industry Traceback Group (“ITG”) best practices and requests from the FCC and other law enforcement agencies. Our standard escalation procedures will ensure all traceback requests are responded to within 24 hours in accordance with FCC requirements.

Solutionreach investigates suspicious activity discovered through the monitoring of its systems or reported to it by customers or third parties, which may result in blocking use of its services.

TCPA Compliance: All outbound calls initiated by Solutionreach are conducted in compliance with TCPA regulations. This includes obtaining proper consent, honoring do-not-call requests, and providing clear identification of the caller.

Certification and Prior Actions

Solutionreach has not been prohibited from filing in the RMD and no prior certifications have been removed. On December 10, 2024, Solutionreach received notice from the Commission that its RMD filing was deficient for failure to include a documented RMP. That oversight has been corrected with this RMP.

Updates

As industry standards evolve to combat and mitigate the effects of illegal robocalls, this RMP will be adapted and improved. In the event of any material change to this RMP, Solutionreach will inform its relevant employees and will file an update to the FCC RMD within ten (10) days of such material change.