



Robocall Mitigation Plan

Business Information

SaaS Labs US, Inc.
355 Bryant Street, #403
San Francisco, CA 94107

Contact Information

Attn: Legal Department
legal@saaslabs.co

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outlines "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider" procedures;
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

SaaS Labs US, Inc. ("SaaS Labs") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. Because SaaS Labs lacks control of the infrastructure necessary to implement STIR/SHAKEN, it is not required to be STIR/SHAKEN compliant. In compliance with the R&O, SaaS Labs submits this RMP and certification.

Know Your Customer

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a

business relationship with SaaS Labs in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

At the time of sign-up, subscribers are required to provide their (a) company name, (b) contact person information, (c) phone number, and (d) information about their business. SaaS Labs also asks for their business websites and social media links, if any. The business website goes through a spam check automatically *i.e.*, it gets a spam score, or a member from the sales team manually checks the website if a spam score cannot be generated. As an additional check, a member of the sales team may go through social media links such as the LinkedIn page of the subscriber and contact person, and/or Instagram page of the subscriber to confirm the presence of the subscriber.

SaaS Labs maintains a list of domains associated with fraudulent accounts. At the time of sign-up, the domains are checked against the list of flagged domains, and the sign-up may be blocked as required. SaaS Labs also maintains a list of credit cards associated with closed fraudulent accounts, and once the credit cards are added to an account, they are checked with the list of flagged credit cards. In addition, SaaS Labs' payment processor helps validate the credit cards that are on file for risk assessment. For any credit card that receives a high-risk score, the associate subscriber account is promptly suspended, and no calling can take place unless and until the subscriber validates its identity, business presence, and its use case.

Acceptable Use Policy

SaaS Labs maintains an Acceptable Use Policy ("AUP") that subscribers must agree to before being permitted to use its network. A link to the AUP is here: www.justcall.io/terms-and-conditions.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59* (Rel. May 19, 2023) ¶¶ 49-51, SaaS Labs provides the following information concerning its upstream voice service carriers.

SaaS Labs upstream providers are:

Twilio Inc.
101 Spear Street, 5th Floor
San Francisco, CA 94105
Evan Finn Purtill
support@twilio.com

Telnyx
515 N State Street, 14th Floor
Chicago, IL 60654
support@telnyx.com

SaaS Labs' service agreement with Telnyx and Twilio does not contain a provision in which Telnyx and Twilio will provide attestation for calls to SaaS Labs' network. However, there are verbal assurances of providing attestations and assurances of providing attestations mentioned in the Help articles. SaaS Labs and both of its upstream providers work together to mitigate all illegal

robocalls, including cooperating fully when receiving traceback requests. SaaS Labs upstream providers are listed as STIR/SHAKEN compliant in the Robocall Mitigation Database.

Monitor Traffic with Analytics & Investigating Suspicious Activity

SaaS Labs has in-house detection services that notify us of suspicious activity (typically indicated by certain calling patterns) once detected. Upon notification, a team member promptly analyzes the call detail records or calls to assess whether the subscriber is engaging in any illegal calling. If the suspicious calls are confirmed, the account is promptly suspended and a member may reach out to the subscriber for business registration, and business use case documentation.

Along with the in-house measures, SaaS Labs collaborates with its upstream providers to prevent any illegal calling. In the event an upstream provider detects or receives any complaint of illegal calling, we proceed to immediately suspend, and investigate the call detail records or calls. If the call detail records confirm the suspicious call activity or calling patterns, SaaS Labs takes immediate steps to ensure further illegal calling does not take place including requesting for use case documentation and/or terminating the subscriber's account.

In addition, SaaS Labs has default disabling calling into areas that are deemed high-risk by our upstream providers. If a subscriber wants to continue calling it is required to submit business registration and business use case documents which are manually checked by our team.

SaaS Labs will implement any Do Not Originate requests it receives from the ITG. SaaS Labs will also cooperate with the Investigative Bodies and document requests and actions taken in response thereto.

No third-party vendors are involved in deploying SaaS Labs' analytics.

Blocking

SaaS Labs will implement Do Not Originate requests it receives from the ITG. SaaS Labs has mechanisms to automatically block suspicious calls using internal analytics. If SaaS Labs' monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, SaaS Labs will take appropriate action which may include suspending or terminating the subscriber's use of SaaS Labs' services. SaaS Labs will cooperate with Investigative Bodies. The point of contact for receiving all traceback requests, Do Not Originate requests and any other investigations is:

Attn: Legal Department; legal@saaslabs.co

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. SaaS Labs will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, SaaS Labs will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification

I, Gaurav Sharma, Chief Executive Officer of SaaS Labs US, Inc. ("SaaS Labs") do hereby certify, under penalty of perjury, the following:

- a. SaaS Labs is not required to implement STIR/SHAKEN, due to its lack of control over the necessary infrastructure.
- b. SaaS Labs business name and primary address are as follows:

SaaS Labs US, Inc.
355 Bryant Street, #403
San Francisco, CA 94107
- c. SaaS Labs has one d/b/a: JustCall.
- d. SaaS Labs has not previously used any other business name.
- e. The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- f. There are two individuals/entities with 10% or more ownership in SaaS: (1) Gaurav Sharma; and (2) Base10 Partners II, L.P. SaaS Labs has three subsidiaries: (1) SaaS Labs Software Private Limited; (2) Atolia SAS; and (3) CallPage.
- g. SaaS Labs' role in the call chain is that of a voice service provider with no STIR/SHAKEN implementation obligation.
- h. SaaS Labs is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. SaaS Labs has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. SaaS Labs is not required to, and does not have, an Operator Code Number.

DocuSigned by:
Gaurav Sharma
623DF0C48A1A48E...

Gaurav Sharma