

Robocall Mitigation Plan

Business Information

smrtStudio Global Inc.
9450 SW Gemini Dr.
PMB 86705
Beaverton, OR 97008

Contact Information

Sebastian Nitu
Compliance Manager
(856) 446 0672
sebi@smrtphone.io

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;
- 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

smrtStudio Global Inc. ("SGI") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. SGI is fully STIR/SHAKEN compliant. In accordance with the R&O, SGI submits this RMP and certification.

Know Your Customer ("KYC")

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 SGI in which we transmit, originate, and/or terminate calls on behalf of the subscriber.

SGI utilizes an extensive KYC program:

Account Creation (Pre-verification):

- Required fields: First and Last Name, Company Name, Phone Number, Email, CRM, and Country.
- Subscribers must explicitly accept our Terms & Conditions, Cancellation Policy, Refund Policy, and Privacy Policy.

Accounts are limited to a maximum of 15 calls before identity verification is mandatory.

- Subscribers are required to provide government-issued identification (ID, Passport, or Driver's License) and a live photo ("selfie").
- Stripe, our payment processor, performs identity verification before the subscriber may continue using the service.
- Access to certain products is completely blocked until verification is complete.

Once identity is confirmed, the subscriber must provide:

- Legal Business Name
- EIN Number
- Business Type & Industry
- Business Website & Address
- At least one designated Business Representative

This layered process (account vetting, ID verification, and business profile validation) ensures that SGI knows its subscriber thoroughly and prevents unauthorized or anonymous use of its system

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. SGI's upstream providers and contact persons/information are as follows:

Twilio Inc
101 Spear Street
1st Floor
San Francisco, CA 94105
Tomislav Nemcic
email address: tnemcic@twilio.com

Telnyx LLC
515 N State St.
14th Floor
Chicago, IL 60654
Shreya Chaudhury
email address: shreya@telnyx.com

Monitoring With Analytics & Investigating Suspicious Activity

SGI takes multiple steps to prevent illegal robocalls from originating on our network. SGI monitors high-volume traffic in partnership with upstream carriers to identify suspicious patterns consistent with illegal robocalls. A Compliance Taskforce manages enforcement, alongside procedures for phishing mitigation and Do Not Call list scrubbing. As delineated herein, SGI has a strong KYC onboarding procedures, as well as a strict Acceptable Use Policy ensure only legitimate subscribers gain access. When suspicious activity is detected, SGI investigates immediately and, if confirmed, take corrective action such as traceback initiation, Caller ID validation, suspension, or termination of accounts. Specific actions include:

- CDR Analysis: Review recent and historical call detail records and compare with expected traffic trends.
- Account Review: Check recent account activity and purchases.
- System Check: Verify no system issue is generating anomalies.
- Path Validation: Confirm call origination paths are valid.
- Direct Subscriber Contact: Reach out to the subscriber to validate use cases and confirm legitimacy.

No third-party vendors are involved in deploying SGI's analytics.

SGI follows Industry Traceback Group ("ITG") recommended best industry practices and cooperates with ITG, the FCC, and law enforcement entities in traceback investigations. To allow for timely and comprehensive responses, SGI devotes sufficient resources to provide prompt and complete resources to traceback requests. SGI certifies that it will respond to all traceback requests within 24 hours of receiving same.

Blocking

SGI has implemented Do Not Originate requests it receives from the ITG DNO Registry. SGI works internally to block suspicious calls. If SGI identifies suspected robocalling patterns that are confirmed with further investigation, SGI will take appropriate action which may include suspending or terminating the subscriber's use of SGI's network.

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. SGI 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, SGI 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 of Sebastian Nitu

I, Sebastian Nitu, Compliance Manger of smrtStudio Global Inc. ("SGI") do hereby certify, under penalty of perjury, the following:

- a. SGI has fully implemented STIR/SHAKEN in the IP portion of its network.
- b. SGI's business name and primary address are as follows:

smrtStudio Global Inc.
9450 SW Gemini Dr.
PMB 86705
Beaverton, OR 97008
- c. SGI's DBA is smrtPhone.
- d. SGI has no previous DBAs.
- 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. The entities with 10% or more ownership in SGI are: Vlad Pustiu, Jordan Samuel Fleming, Alexandru Parge, and Stefan Parge. SGI has no affiliates or subsidiaries.
- g. SGI's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation.
- h. SGI is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. SGI has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. SGI's Operator Code Number is 477K.



Sebastian Nitu

