

Robocall Mitigation Plan

Grasshopper Group, LLC

Business Information

Grasshopper Group, LLC
333 Summer Street, 5th Floor
Boston, MA 02210

Contact Information

Lauren Phizicky
Senior Legal Counsel
438-816-9299
telecom@goto.com

Overview and Purpose

In the Commission's recent 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, outline "reasonable steps" taken to avoid originating illegal robocalls.

Grasshopper Group, LLC (the "Company") has fully implemented STIR/SHAKEN requirements.

The purpose of this document is to explain the additional steps the Company has taken to avoid originating illegal robocalls, including the following:

- "know your customer" procedures;
- 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.

Know Your Customer ("KYC")

New subscribers to the Company's service must provide name, telephone number, email address, business civic address, and valid credit card information.

The Company operates a fraud prevention program that proactively monitors customer accounts for various indicia of potentially illegal or fraudulent activity. Some metrics lead to systematic account closure or outbound call blocking, whereas others result in accounts being flagged for further investigation or review. Examples of factors reviewed include credit card validation, civic address review, the nature of the account email address and its apparent connection to the given name of the business, and IP address location.

The Company offers a free trial version of its service which has a lower KYC threshold, but it has accordingly restricted free trial users to just 50 minutes of outbound calls.

The Company continues to refine its processes to respond to changing behavior and patterns in its efforts to avoid giving access to its services to bad actors in the first place and to promptly remove such access when illegal activity is discovered. To this end, the Company participates in industry associations to learn best practices from domain experts and law enforcement entities.

Know Your Upstream Providers

The Company is an originating provider that sends its customers' call traffic to downstream providers. The Company does not transit calls as a "carrier" for other providers.

However, the Company does monitor and limit inbound call rates on a per-number basis to help prevent excessive inbound volumes clearly indicative of robocalls.

Also, the Company works closely with downstream carrier providers to share best practices and to respond to any illegal activity detected beyond the Company's own network. Escalations from downstream carrier partners are addressed by the Company promptly, including by Company staff who remain "on call" and reachable during non-business hours to address certain escalations.

Acceptable Use Policy ("AUP")

The Company maintains and enforces an AUP that subscribers must agree to before being permitted to use its services. The AUP requirements and prohibitions are located in various parts of the Company's online terms and include, other things, prohibition against:

- using the services for any illegal purposes;
- providing false or deceptive information intended to impersonate another; and
- using the services to engage in, or in connection with, fraudulent activities.

Violation of these prohibitions constitute grounds for account termination.

The Company's terms also allow for blocking of calls or call destinations believed to be associated with high-frequency machine dialing.

Telephone Number Authorization

The Company directly manages the telephone numbers ("TNs") used by its subscribers and tracks these numbers in its inventory system and monitors the assignment of these numbers. TN validation upon call initiation is inherent in the Company's call initiation processes.

The Company does not allow a customer to display a caller identity for a TN that Company has not supplied.

Analytics for Monitoring Traffic

The Company works to detect a calling pattern consistent with illegal robocalls. Various call metrics and thresholds are observed, including metrics regarding outbound call rates and destinations, and if thresholds are surpassed, the Company will either automatically block calls or else flag the account for more detailed investigation.

When illegal calls are identified, the Company takes appropriate action, which typically involves suspending or terminating the party's ability to originate calls on the Company's network.

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

Investigate Suspicious Activity

When automated traffic analysis indicates the presence of possible illegal robocalling but does not automatically trigger call blocking, this pattern is highlighted on an actively monitored dashboard and the Company's fraud prevention team will be alerted. Investigation by the fraud team may include (but is not limited to):

- checking call detail records and benchmarking against expected trends;
- additional analysis of KYC information;
- checking recent and past account activity and purchases;
- contacting the subscriber – often incognito – to understand their use case and validate that the activity belongs to that subscriber.

The Company also participates in Industry Traceback Group ("ITG") traceback investigations. To allow for timely and comprehensive responses, the Company has streamlined and centralized its processes for responding to traceback requests and will devote the required resources to respond efficiently, as required.

Blocking

The Company has mechanisms in place to automatically block suspicious calls using internal analytics in certain circumstances. If the Company's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, it will take appropriate action which typically include suspending or terminating the subscriber's use of the Company's services.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. The Company 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, the Company 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 Michael Donahue

I, Michael Donahue, Chief Legal Office and Secretary of Grasshopper Group, LLC ("Company"), do hereby certify, under penalty of perjury, the following:

- (1) Company has fully implemented STIR/SHAKEN in the IP portions of its network.
- (2) Company's business name and primary address are as follows:

Grasshopper Group, LLC
333 Summer Street, 5th Floor
Boston, MA 02210
- (3) Company has no other business names in use.
- (4) Company has no previously used business names.
- (5) 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.
- (6) The following persons/entities own more than 10% of Company each: GoTo Technologies USA, LLC (100% owner).
- (7) The following persons are Company's officers: Michael Rubin; John Joseph Markey II, Michael J. Donahue.
- (8) Company has the following subsidiaries/affiliates: parent as mentioned above; GoTo Communications, Inc. is an affiliate also filing an RMP.
- (9) None of the persons/entities in items 5 – 7 above have had their license denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (10) Company's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (11) Company has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (12) Company is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (13) Company's Operator Code Number is 403K.

Michael J. Donahue