

Robocall Mitigation Plan

Business Information

Telengy, LLC.
11 Broadway – Suite 1015
New York, NY 10004

Contact Information

Stephen Irwin
VP of Operations
(646) 547-5700
stephen@telengy.net

Overview

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, 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";
- 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

Telengy, LLC. ("Telengy") is a VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. Telengy is fully STIR/SHAKEN compliant. In compliance with the R&O, Telengy 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 Telengy in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

New Subscribers

[REDACTED]



All subscribers are required to provide account information including (but not limited to) name, company name, location, phone number, email address, website address, payment method, tax ID, etc.

Existing Subscribers



Acceptable Use Policy

Telengy maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use Telengy's network. Among other things, this AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law;
- violating applicable industry accepted guidelines; and
- using Telengy's service to engage in (or in) connection with fraudulent activities.

Telengy's contractual terms with subscribers specify that Telengy may take action, up to suspension or termination of service for violation of the AUP.

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, Telengy provides the following information:

Telengy has no upstream providers. It receives its numbers directly from NANPA and originates voice traffic.

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the subscriber. In most cases, Telengy directly manages the TNs used by its subscribers. Telengy tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Telengy's assignment of the TN to its subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by Telengy, then TN validation is necessary. Subscribers are required to either submit documentary evidence and/or complete a proprietary verification process prior to being given the ability to use a TN not directly managed by Telengy on outbound PSTN calls. On outbound PSTN calls, Telengy's

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

Telengy actively participates in Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Telengy devotes sufficient resources to provide prompt and complete resources to traceback requests.

Telengy will investigate suspicious activity found by its monitoring systems or reported to Telengy by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Telengy contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform.

For all new and renegotiated Telengy contracts governing the transport of voice calls, Telengy will use best efforts to contractually require Telengy's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Telengy will implement Do Not Originate requests it receives from the ITG. If Telengy's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Telengy will take appropriate action which may include suspending or terminating the subscriber's use of Telengy's network. Telengy will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement, the state attorney general's office, etc.), to the FCC and/or the ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Telengy 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, Telengy 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 Stephen Irwin

I, Stephen Irwin, Vice President of Operations of Telengy, LLC. ("Telengy") do hereby certify, under penalty of perjury, the following:

- a. Telengy has fully implemented STIR/SHAKEN in the IP portions of its network. Telengy directly signs all its calls.
- b. Telengy's business name and primary address are as follows:

Telengy, LLC.
11 Broadway – Suite 1015
New York, NY 10004

- c. 
- d. None of the persons/entities listed above have had licenses revoked by the FCC or have been subject to FCC enforcement actions.
- e. Telengy does not have any other business name.
- f. Telengy has not previously used any other business name.
- g. 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.
- h. Telengy's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation to serve end-users.
- i. Telengy has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- j. Telengy is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- k. Telengy's Operator Code Number is 148J.


Stephen Irwin