

Robocall Mitigation Plan

Business Information

Cytracom, LLC
450 Century Parkway
Suite 100
Allen, TX 75013

Contact Information

Benjamin L. Booth
CFO
469.777.4644
legal@cytracom.com

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";
- 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

Cytracom, LLC ("Cytracom") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. As certified in the FCC's Robocall Mitigation Database, Cytracom has fully implemented STIR/SHAKEN. In compliance with the R&O, Cytracom 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 Cytracom in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Cytracom's KYC program involves obtaining specific subscriber information when the subscriber is onboarded. This process includes collecting such information such as:

- physical business location; and
- contact person(s).

Acceptable Use Policy ("AUP")

Cytracom maintains an AUP that subscribers must sign before being permitted to use Cytracom's system. Among other things, the 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; and
- using Cytracom's service to engage in or in connection with fraudulent activities.

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

Know Your Upstream Provider

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, Cytracom provides the following information concerning its upstream voice service carrier:



Cytracom's agreement with its upstream provider contains no provision specific to robocall mitigation. Cytracom has, however, received assurances from Bandwidth that it has, and will continue to, sign calls transmitted to Cytracom, and will work closely with Cytracom to mitigate illegal robocall traffic.

Monitor Traffic With Analytics

Cytracom works with its upstream carrier to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. If Cytracom detects a calling pattern consistent with illegal robocalls, we will identify the party and will appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our system.

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

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Cytracom's technical operations team is alerted which follows the defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

Cytracom is familiar with, and uses best efforts to follow the Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Cytracom will devote sufficient resources to provide prompt and complete resources to traceback requests.

Blocking

Cytracom will implement Do Not Originate requests it receives from the ITG. Cytracom has procedures to block suspicious calls. If Cytracom identifies suspected robocalling patterns that are confirmed with further investigation, Cytracom will take appropriate action which may include suspending or terminating the subscriber's use of Cytracom's system. Cytracom will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement, 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 response to the dynamic nature of mitigating illegal robocalling. Cytracom 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, Cytracom 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 Benjamin L. Booth

I, Benjamin L. Booth, CFO of Cytracom LLC ("Cytracom") do hereby certify, under penalty of perjury, the following:

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

Cytracom, LLC
450 Century Parkway
Suite 100
Allen, TX 75013

- c. Cytracom has no other business names in use.
- d. Cytracom 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. [REDACTED]
- g. Cytracom's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- h. Cytracom and its interest holder have not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. Cytracom and its interest holder have not subject been to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. Cytracom's Operator Code Number is 177K.

DocuSigned by:

Ben Booth

Benjamin L. Booth