



Robocall Mitigation Plan

Business Information

CloudCall Inc.
268 Summer Street
Boston, MA 02210, USA

Contact Information

Paul Williams
Chief Finance Officer
Paul.williams@cloudcall.com

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, outline "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;
- 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

CloudCall Inc. ("CloudCall") is a VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network.

As certified in the FCC's Robocall Mitigation Database, CloudCall has fully implemented STIR/SHAKEN. In compliance with the R&O, CloudCall 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 that subscriber. A subscriber is an entity that has a business relationship with CloudCall in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

CloudCall conducts basic background checks to ensure client companies are validly incorporated. CloudCall checks social media accounts and only accepts payment from credible banks.

CloudCall's KYC program involves obtaining specific subscriber information when payment is made for services. This process includes collecting such information such as:

A handwritten signature in black ink, appearing to be "Paul Williams".

- physical business location;
- contact person(s);
- nature of the customer's business.

CloudCall is a small company, we have a small number of customers. We know our customers and understand their use cases.

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, CloudCall provides the following information concerning its upstream voice service carriers.

CloudCall has two upstream providers from which it receives voice traffic:

- 1) Bandwidth Inc.
900 Main Campus Drive
Suite 100
Raleigh NC 27606
Stephen Thayer
voicsecurity@bandwidth.com
- 2) Inteliquent, Inc. (d/b/a Sinch)
550 W. Adams St.
Suite 900
Chicago IL 60661
Stacy Graham
stacy.graham@sinch.com

CloudCall has master service agreements with its upstream providers. CloudCall and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

CloudCall maintains an AUP that subscribers must agree to before being permitted to use CloudCall's software and services. Among other things, the AUP prohibits:

- using our service for any illegal purposes whatsoever;
- engaging in activity for which FCC or any equivalent national regulatory authority, has restricted or regulated in relation to proper use of the public telephony network or the Internet;
- using our service if CloudCall determines, at its sole discretion, that its provision for this customer is prohibited by applicable law or has become impractical or unfeasible for any legal or regulatory reason; and
- using our service to offer or otherwise make available to others fraudulent goods, services, schemes, or promotions, including make-money-fast schemes, Ponzi and pyramid schemes, phishing, pharming, harvesting or similar deceptive practices.

Analytics for Monitoring Traffic

CloudCall works to detect a calling pattern consistent with illegal robocalls. If such a call is detected, we will identify the party that is using our network to originate those calls and will take 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 network.

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

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, CloudCall's risk prevention 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.

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

Blocking

CloudCall will promptly respond to Do Not Originate requests it receives from the ITG. CloudCall has mechanisms to automatically block suspicious calls using internal analytics. If CloudCall's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, CloudCall will take appropriate action which may include suspending or terminating the subscriber's use of CloudCall's network. CloudCall will cooperate with investigative bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), to the FCC, and/or the ITG; as well as documenting requests and 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. CloudCall will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

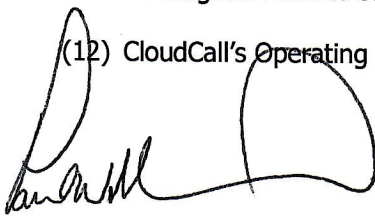
In the event of any material change to this plan, CloudCall will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Paul Williams

I, Paul Williams, Chief Finance Officer, of CloudCall, do hereby certify, under penalty of perjury, the following:

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

CloudCall, Inc.
268 Summer Street
Boston, MA 02210, USA
- (3) CloudCall has no other business names in use.
- (4) CloudCall has not previously used any other business name.
- (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) CloudCall US Group, Inc. owns more than 10% of CloudCall and is its parent company.
- (7) The following persons are CloudCall's directors/officers: Paul Williams (CFO), and Simon Cleaver.
- (8) None of the persons/entities in items 5 – 6 above have had their licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (9) CloudCall's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (10) CloudCall has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (11) CloudCall is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (12) CloudCall's Operating Company Number is 807K.



Paul Williams