

Robocall Mitigation Plan

Business Information

Cloud Compliance Solutions, Inc.

7551 Wiles Road Suite 106

Coral Springs, FL 33067

Contact Information

Kelley R. Allen CEO- 561-451-5488

kallen@ccsius.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, 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;
- "know your upstream provider" 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

Cloud Compliance Solutions Inc. ("CCSI") is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network. CCSI is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, CCSI has been exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as CCSI now file RMPs. This document delineates CCSI's RMP. Because CCSI does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As

delineated herein, CCSI works closely with its upstream provider to carry out the required mitigation functions.

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

CCSI's KYC program involves obtaining specific information when a subscriber signs up for service. This process includes collecting such information such as:

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

Acceptable Use Policy "AUP".

CCSI maintains an AUP that subscribers must agree to when being permitted to use CCSI's network. 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;
- violating applicable industry accepted guidelines; and
- using CCSI's service to engage in or in connection with fraudulent activities.

CCSI's contractual terms with subscribers specify that CCSI may suspend or terminate 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) ,i,i 49-51, CCSI provides the following information concerning its upstream voice carrier.

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

Bandwidth, Inc.

2230 Bandmate Way

Raleigh, NC 27607

855-290-8135

Telnyx, LLC.

515 N. State Street

Chicago, IL 60654

Analytics for Monitoring Traffic

CCSI works with its upstream provider to identify behaviors which indicate illegal call activity.

Examples of calling patterns monitored:

- anomalies in cost generated by calls from a single customer;
- multiple overlapping calls on the same account is a risk of not having a single subscriber using the service;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level); and
- anomalies in call duration distribution (most calls having similar duration is not representative for residential service usage).

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, CCSI works with its upstream provider to follow 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 particular use case and validate that the activity belongs to that subscriber.

Because CCSI does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in CCSI's analytics.

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

CCSI works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to CCSI by subscribers or third parties. The investigation could potentially result in opening a traceback request or with CCSI contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream provider to block their use of the platform.

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

Blocking

CCSI will implement Do Not Originate requests it receives from the ITG. CCSI's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If CCSI and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, CCSI will take appropriate action which may include suspending or terminating the subscriber's use of CCSI's service. CCSI will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorney general's office), as well as 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. CCSI 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, CCSI 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 Kelley R. Allen

I, Kelley R. Allen, CEO of CCSI, Inc. ("CCSI"), do hereby certify, under penalty of perjury, the following:

- (1) CCSI, by virtue of its status as a "pure reseller" does not have access to the necessary infrastructure to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.
- (2) CCSI's Business name and primary address are as follows:
Cloud Compliance Solutions, Inc.
7551 Wiles Road, Suite 106
Coral Springs, FL 33067
- (3) Other than those listed in the above robocall mitigation plan, CCSI has no other business names in use.
- (4) CCSI has not previously used any other business name.
- (5) Kelley R. Allen is the majority owner and principal of CCSI.
- (6) CCSI has no subsidiaries.
- (7) CCSI has no affiliates.
- (8) None of the persons/entities in items 5 - 7 above have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (9) 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.
- (10) CCSI's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (11) CCSI has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (12) CCSI is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (13) CCSI's is not required to, and does not have, an operating company number.

Kelley R. Allen



Date: December 21, 2024