

Robocall Mitigation Plan

Business Information

Avaya Cloud Inc
350 Mount Kemble Ave.
Morristown, NJ 07960

Contact Information

Laura Jones
Officer
703-390-8347
lhjones@vaya.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" procedures;
- 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

Avaya Cloud Inc. ("Avaya") is a VSP dedicated to stopping illegal calls from originating in our network. As certified in the FCC's Robocall Mitigation Database, Avaya has fully implemented STIR/SHAKEN in the IP portion of its network. In compliance with the R&O, Avaya submits this RMP and certification.

Know Your Customer

Avaya provides its services to enterprise customers ("Customers"). Avaya obtains and records; information to determine the identity of its Customers, such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the Customer's business. Customers are required to promptly notify Avaya of updates to such information, including, but not limited to the physical location of its users.

Acceptable Use Policy

Avaya maintains an Acceptable Use Policy ("AUP") that includes provisions in its standard customer agreements allowing for suspension of its Customers' right to use the services or terminate the terms and conditions upon notice if: (i) a Customer violates, or Avaya has reason to believe that a Customer has violated, any provision of Avaya's Acceptable Use Policy which is available at the following site: <http://support.avaya.com/TermsOfSale>; (ii) there is an unusual spike or increase in a Customer's use of the service, and there is reason to believe such traffic or use is fraudulent or negatively impacting the operating capability of the service; and (iii) Avaya's provision of the service to Customer is prohibited by applicable law, or has become impractical or unfeasible due to any legal or regulatory change.

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, Avaya provides the following information concerning its upstream voice carrier.

Avaya has one upstream provider from which it receives voice traffic:

Telnyx, LLC
311 West Superior St
Suite 504
Chicago IL 60654
Olive Morris
(312) 945-7420
olive@telnyx.com

Avaya's master service agreement with its upstream provider contains provisions regarding robocall mitigation, *i.e.* that the carrier abides by all the FCC's robocall mitigation rules.

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 Customer. A Customer is permitted to use a TN as a caller identity if a TN is directly managed by Avaya and/or obtained by Avaya from one of Avaya's underlying carriers for use by the Customer. In most cases, Avaya directly manages the TNs used by its Customers. Avaya tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Avaya's assignment of the TN to its Customer.

If a Customer wishes to use a TN as a caller identity and that TN is not directly managed by Avaya, then TN validation is necessary. If a Customer's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, Avaya will attest calls originated with these TNs.

When originating a call, Avaya checks the calling party number against Avaya's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

Analytics for Monitoring Traffic

Dynamic Traffic Analysis identifies 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 Customer 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).

The only third-party vendor involved in deploying Avaya's analytics is Telnyx, LLC.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our risk prevention team is alerted which follows the defined procedures on investigating such Customers.

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 Customer to understand his particular use case and validate that the activity belongs to that Customer.

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

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

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

Blocking

Avaya will implement Do Not Originate requests it receives from the ITG. Avaya has mechanisms to automatically block suspicious calls using internal analytics. If Avaya's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Avaya will take appropriate action which may include suspending or terminating the Customer's use of Avaya's network. Avaya 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) 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 response to the dynamic nature of mitigating illegal robocalling. Avaya 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, Avaya 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 Lynne Pelletier

I, Laura Jones, Officer for Avaya Cloud Inc. ("Avaya"), do hereby certify, under penalty of perjury, the following:

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

Avaya Cloud Inc
350 Mount Kemble Ave.
Morristown, NJ 07960

3. Avaya has no other business names in use.
4. Avaya has not previously used any other business name.
5. Avaya is 100% owned by Avaya LLC; Avaya Corp. is the parent company of Avaya LLC.
6. 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.
7. Avaya's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
8. Avaya has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
9. Avaya is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
10. Avaya's Operator Code Number is 219K.

DocuSigned by:

Laura Jones

6D851EA089E64C7...

Laura Jones
Officer
Avaya Cloud Inc.