

Robocall Mitigation Plan

Business Information

Zoho Corporation
4141 Hacienda Dr.
Pleasanton, CA 94588

Contact Information

Kumaravel Natarajan
Product Head
888-900-9646
kumaravel@zohocorp.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

Zoho Corporation ("Zoho") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. In compliance with the R&O, Zoho 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 Zoho in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

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

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

- nature of the customer’s business.

Acceptable Use Policy (“AUP”)

Zoho maintains an AUP that subscribers must agree to before being permitted to use Zoho’s network. Zoho’s AUP may be found here: <https://www.zoho.com/voice/terms.html>

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, Zoho provides the following information concerning its upstream voice service carriers:

Bandwidth, Inc.
2230 Bandmate Way,
Raleigh, NC 27607
Luke Stowers
lstowers@bandwidth.com

Telnyx, LLC
311 West Superior St
Suite 504
Chicago IL 60654
Olive Morris
regulatory@telnyx.com

NTT Cloud Communications U.S. Inc.
5 Concourse Parkway NE
Suite 1600
Atlanta GA 30328
David Mileusnich
DAVID.MILEUSNICH@GLOBAL.NTT

AVOXI, Inc.
300 Galleria Parkway
Suite 1040
Atlanta GA 30339
Weston Edmunds
weston@avoxi.com

Zoho and its upstream providers have agreed to work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Telephone Number Authorization

A Telephone Number (“TN”)-based caller identity is the originating phone number included in call signaling used to identify an outbound caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Zoho and/or obtained by

Zoho from one of Zoho's underlying carriers for use by the subscriber. In most cases, Zoho directly manages the TNs used by its subscribers. Zoho tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Zoho'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 Zoho, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, Zoho will attest calls originated with these TNs.

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

Monitoring With Analytics

Zoho works with its upstream carrier to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. If Zoho detects a calling pattern consistent with illegal robocalls, we will identify the party 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 system.

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

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Zoho follows certain 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 unusual 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.

Zoho follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Zoho devotes sufficient resources to provide prompt and complete resources to traceback requests. Zoho will respond to traceback requests within 24 hours of being notified of same.

Blocking

Zoho will implement Do Not Originate requests it receives from the ITG. Zoho works with its upstream carriers to block suspicious calls. If Zoho and/or its upstream carriers identify suspected robocalling patterns that are confirmed with further investigation, Zoho will take appropriate action which may include suspending or terminating the subscriber's use of Zoho's network. Zoho will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), and the FCC, 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. Zoho 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, Zoho 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 Kumaravel Natarajan

I, Kumaravel Natarajan, Product Head of Zoho Corporation (“Zoho”) do hereby certify, under penalty of perjury, the following:

- a. Zoho’s business name and primary address are as follows:

Zoho Corporation
4141 Hacienda Dr.
Pleasanton, CA

- a. Zoho has no d/b/a name.
b. Zoho has not previously used any other business names.
c. 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.
d. The following persons own 10% or more of Zoho: Radha Vembu, Product Manager; Sekar Vembu, Founder. Zoho’s Principals are: Sridhar Vembu, Radha Vembu, and Sekar Vembu. Zoho has no subsidiaries or affiliates.
e. Zoho’s role in the call chain is that of a voice service provider that is exempt from STIR/SHAKEN implementation due to its lack of control over the necessary infrastructure.
f. Zoho is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
g. Zoho has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
h. Zoho is not required to, nor does it have, an Operator Code Number.



Kumaravel Natarajan