

# **Robocall Mitigation Plan**

## **Business Information**

Zendesk, Inc.  
181 Fremont Street, 17th Floor,  
San Francisco, CA 94105

## **Contact Information**

John Didday  
Associate General Counsel, Product & Privacy  
+1 (445) 263-0535  
[productlegal@zendesk.com](mailto:productlegal@zendesk.com)

## **Overview**

In the Federal Communications Commission's ("FCC") 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 providers, regardless whether they have the facilities necessary to implement STIR/SHAKEN, must take "reasonable steps" to mitigate illegal robocall traffic, and file a Robocall Mitigation Plan ("RMP") outlining these steps in the FCC's Robocall Mitigation Database ("RMD").

In addition to the "reasonable steps", the FCC requires that an RMP include:

- "Know your customer" procedures;
- "Know-your-upstream provider";
- A description of any call analytics systems 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 stated that an RMP is sufficient if it includes detailed practices that can reasonably be expected to significantly reduce the origination of illegal robocalls and the voice service provider ("VSP") complies with the practices described in its filing. Zendesk's RMP that is discussed below does just that.

## **Summary of Zendesk's Voice Services and RMP Purpose**

Zendesk, Inc. ("Zendesk") is a customer support software-as-a-service company offering a platform that powers interactions between customer support agents and their end customers across various channels such as email, chat, social media, and, relevant here, traditional telephone support.

Zendesk enables its customers to purchase phone numbers—resold from its upstream provider, [Twilio, Inc.](#) ("Twilio")—for use within its integrated customer support platform. Calls

can be recorded, transcribed, and stored within the customer's Zendesk instance, with these interactions integrated with other supported channels. This solution, known as "Zendesk Voice" (formerly "Zendesk Talk"), is primarily used for inbound calls from end customers, though outbound calling functionality via Twilio is also available to accommodate certain outbound support scenarios (such as a call back).

While Zendesk sells phone numbers and minutes for Zendesk Voice, Twilio's platform handles all routing, calls, recording, and the Voice infrastructure. Zendesk combines Twilio's services with features like transcription and summarization, integrating them into the Zendesk customer support platform. Zendesk does not have an Operating Company Number ("OCN").

Zendesk is dedicated to preventing illegal calls from originating in its network and monitoring traffic passing through it. As a reseller or value-added service provider ("VASP"), Zendesk does not have control over the network infrastructure facilities necessary to implement STIR/SHAKEN. In compliance with the R&O, Zendesk submits this RMP.

### **Know Your Customer ("KYC")**

The accurate identification of a customer in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that customer. A customer is an entity that has a business relationship with Zendesk in which we transmit, originate, and/or terminate calls on behalf of the customer.

Zendesk's KYC procedures involve obtaining specific customer information when payment is made for its services. This process includes collecting information, such as:

- Business name;
- Physical business address;
- Contact person(s);
- Email address;
- Billing information; and
- Nature of the customer's business.

In addition, Zendesk regularly conducts customer screenings to review potential affiliations with sanctioned or black-listed entities or individuals.

### **Acceptable Use Policy**

Zendesk maintains a [User Content and Conduct Policy](#) ("UCCP") and other binding terms that customers must agree to before being permitted to use Zendesk's software. Among other things, the UCCP and other binding terms prohibit the use of Zendesk products and services to:

- send or host spam, including the sending of unwanted or unauthorized commercial content, unwanted or mass solicitation, or other forms of duplicative or unsolicited messages;
- engage or directly or indirectly promote illegal, or fraudulent activities;
- engage in abusive, harassing, or bullying behavior, including a prohibition on illegal dissemination of private information or media using the services; and
- deceive individuals or impersonate third parties.

Zendesk's contractual terms with customers specify that Zendesk may take action, up to suspension or termination of service for violation of the UCCP or other binding terms.

### **Know-Your-Upstream Providers**

In accordance with the FCC'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, Zendesk provides the following information on its upstream voice service provider:

Twilio Inc.  
 101 Spear Street, 1st Floor  
 San Francisco CA 94105  
 United States  
 Paul Kenefick  
 Sr. Counsel, Compliance & Telecom Regulatory  
 (202) 679-7501  
[regulatory-north-america@twilio.com](mailto:regulatory-north-america@twilio.com)

Since Zendesk lacks control over the network infrastructure required to implement STIR/SHAKEN, it relies on Twilio to fulfill the Know-Your-Upstream Provider obligations and ensure that upstream providers are properly listed in the FCC's Robocall Mitigation Database and not delisted due to enforcement actions before accepting traffic. Zendesk and its upstream providers are committed to diligently mitigating illegal robocalls, including fully cooperating with traceback requests.

### **Only Accepting Traffic from Providers that Have Affirmatively Filed in the RMD**

In accordance with FCC rules, because Zendesk is a reseller of VoIP services and lacks the control over the network infrastructure necessary to implement STIR/SHAKEN, Zendesk relies on Twilio, which is currently listed in the RMD, to only accept traffic from providers that at a minimum satisfy the requirements under 47 C.F.R. §§ 64.6305(g)(1)-(4).

## **Monitoring with Analytics**

As a reseller or VASP, Zendesk lacks control over the network infrastructure required to implement STIR/SHAKEN and relies on Twilio to analyze and monitor high-volume traffic for patterns consistent with robocalls. Zendesk does not use a third-party analytics vendor(s).

If suspicious calling patterns are detected by its upstream voice service provider originating from a Zendesk customer, Twilio reports this to Zendesk for further investigation and appropriate action. If the calls are determined to be robocalls or spam calls originating from a Zendesk customer, Zendesk's service to that customer will be suspended or terminated.

## **Investigate Suspicious Activity**

Since Zendesk lacks the control over the network infrastructure necessary to implement STIR/SHAKEN, Zendesk relies on its upstream voice service provider to monitor and detect calling patterns consistent with or specific to illegal robocalls, including large bursts of traffic in small timeframes and reports of spam or unwanted calls being made to end users. If Twilio has good reason to suspect illegal robocalling or illegal spoofing is originating from a Zendesk customer, Zendesk works with Twilio to address and block such traffic. Zendesk's voice services to its customers will be investigated and suspended or terminated, as appropriate and in accordance with Zendesk's UCCP.

Zendesk is committed to promptly responding to all traceback requests from the FCC, law enforcement, and the industry traceback consortium/group ("ITG"), cooperating fully to investigate and stop illegal robocallers from using Zendesk's services and ensure that it is not utilized for the origination, termination or routing of unwanted and illegal robocalls. Zendesk will respond to all traceback requests within 24 hours of being notified of the same.

## **Blocking**

Zendesk works with its upstream provider to block suspicious calls. Since Zendesk lacks the control over the network infrastructure necessary to implement STIR/SHAKEN, if there is an obligation to block calls based on a reasonable Do Not Originate List ("DNO"), Zendesk will rely on its network provider, Twilio, to block such calls on such a list. If Zendesk and/or its upstream provider identify suspected robocalling patterns that are confirmed by further investigation, Zendesk will take appropriate action, which may include suspending or terminating the customer's use of Zendesk's services. Zendesk will cooperate with investigative bodies, including state attorneys general offices, the FCC, and/or the ITG, as well as documenting requests and actions taken in response.

## **Plan Updates**

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Zendesk 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, Zendesk 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.