

ZOOM VOICE COMMUNICATIONS, INC.

ROBOCALL, SCAM CALLING AND FRAUD MITIGATION PROGRAM

PURPOSE

Zoom Voice Communications, Inc. (“Zoom”) is committed to protecting its customers from illegal and spoofed robocalls and has implemented robust measures to identify and stop illegal robocallers from using Zoom Phone to originate such calls. The purpose of this Robocall Mitigation Program (the “Program”) is to outline these measures and ensure organizational alignment on the processes and principles set forth herein. The Program also outlines remedial measures that Zoom will undertake if Zoom Phone is being used to originate illegal and spoofed robocalls or if a Zoom customer alerts Zoom to potential fraudulent activity on their account.

The Program will be reviewed annually and updated as necessary by Zoom to ensure that it remains responsive to current robocalling threats, scam calling threats and fraud mitigation, conforms with applicable law, and addresses any changes to Zoom’s network architecture and services as well as any organizational changes that may occur from time to time.

ZOOM PHONE’S ROBOCALL MITIGATION MEASURES

1. Zoom has implemented the STIR/SHAKEN framework.

a) Underlying Service Providers

Zoom utilizes the VoIP networks of underlying service providers to provide Zoom Phone services. These carrier partners also supply the telephone numbers Zoom Phone issues to customers (and Zoom Phone Customers must complete the forms of our underlying carriers before being issued these numbers, or to port their own numbers). Our service providers are required to pass through the SIP header with the proper attestation for calls originating from Zoom Phone customers to interim or terminating carriers. As of the date of this certification, Zoom has conducted testing with its partners and made the necessary adjustments to enable the authentication and validation of calls through its underlying service providers consistent with the STIR/SHAKEN framework.

b) On Net Calls

At this time, on-net calls (calls carried on the Zoom Phone network that originate with one Zoom Phone customer and terminate with another Zoom Phone customer) are not covered by our underlying carrier attestations. The FCC requires that on-net calls receive attestation and verification in a manner that is “consistent with” the STIR/SHAKEN framework. Because Zoom is both the originating service provider and the terminating service provider for these calls and there would be no SIP header for a handoff in the Trace ID of such calls, Zoom will be adding a green checkmark to these calls as they are routed through to customers when a call is verified and has an A-level attestation. The green checkmark on the on-net calls shall represent A-level attestation from Zoom as the originating network. All Zoom Phone customers calling other Zoom Phone accounts on-net are verified and authenticated in the same way that calls routed through our underlying service providers are verified and authenticated. Zoom intends

to nonetheless incorporate an “attestation” line in the Trace ID for calls originated on net no later than September 28, 2021.

2. Zoom actively monitors its network for robocalling and other suspicious traffic.

Zoom has deployed software and machine learning to analyze voice network traffic to identify and monitor patterns consistent with robocalls. For example, Zoom monitors call duration, calling patterns, and call destinations and conducts internal investigations when unusual patterns are detected. Zoom’s carrier partners also utilize technologies to monitor suspicious traffic. If Zoom or its underlying providers detect patterns that are consistent with illegal robocalls, toll fraud, or other suspicious traffic, Zoom examines the party’s account information and conducts an investigation. Zoom may suspend or terminate such accounts, or take whatever action is appropriate based on its findings.

3. Zoom confirms the identity of its Zoom Phone customers.

Zoom utilizes a combination of rule-based heuristics and machine learning to determine the risk associated with a new account. These are deployed to run in real-time or batch processing, depending on the fraud risk and level urgency. At the Account Registration stage, Zoom monitors and automatically scans new account registrations for suspicious account information. Using several indicators at the account registration stage, Zoom scans the information provided by customers in real time as they register new accounts. Zoom’s account registration fraud detector finds and suspends suspicious accounts soon after creation.

When Zoom provisions telephone numbers (whether directly or through underlying carriers), customers must comply with Zoom’s policies and processes requiring customers to submit information to verify customer identity and rights to numbers being ported, etc. These policies and processes are designed for compliance with the specific know your customer requirements applicable in the relevant jurisdiction.

4. Zoom Phone does not support CLI overstepping or spoofing

Zoom Phone also deploys technologies to ensure that robocallers cannot spoof using a Zoom Phone account. Zoom Phone may only be enabled with a Zoom account and the information provided at the account set up is linked to any numbers issued to the customer (and which customer was verified at the time of account set-up). Any hardware that is linked to the registered customer account cannot be used to spoof, nor can the account holder “change” the number shown on its outbound call, except to reflect information in the Zoom account registration (e.g., main account phone number; main account holder name). In rare instances, exceptions can be made to enable a customer to utilize numbers it owns but cannot port or to address similar irregularities. In such cases, Zoom consults with internal stakeholders to determine whether the exception is permissible and conforms to internal policies and applicable law.

5. Zoom’s customer contracts and terms prohibit usage of Zoom’s services for any illegal purposes, including illegal robocalls, and give Zoom the right to terminate usage in case of violations.

Zoom’s Terms of Use and any negotiated customer contracts contain compliance with laws provisions that prohibit usage for unlawful purposes or usage that is in conflict with applicable laws or regulations. In addition, Zoom Phone’s service description, service terms and policies prohibit usage for unlawful purposes and enable Zoom to terminate a customer’s account for violations of such terms. Zoom exercises these rights, as necessary, to stop illegal robocalling originating from its customers.

6. Zoom has integrated call blocking and labeling features into the Zoom Phone product.

These features are described in detail on various parts of our website: [Managing the Blocked List](#)

7. Robocall Remediation Measures

In connection with its STIR/SHAKEN implementation and robocall mitigation program, Zoom cooperates with its underlying service providers to quickly investigate and suspend or terminate accounts that are found to be originating illegal traffic. Zoom's underlying service providers in the United States each have Acceptable Usage Policies, with which Zoom and Zoom's customers must comply. When an underlying service provider brings potential violations to Zoom's attention, the Zoom DevOps 24/7 NOC Team reviews the request, then the Fraud Team promptly investigates the matter as necessary. If the Fraud Team determines that a Zoom customer is generating suspicious traffic, Zoom notifies the offending customer and may suspend the account, depending upon the circumstances. Zoom may also terminate the customer's account if circumstances warrant termination. The Fraud Team continually iterates and improves on its detection capabilities to address new types of attacks.

8. Cooperation in Traceback Efforts

Zoom is committed to cooperating in traceback investigations involving calls carried on its network or originated by its customers using Zoom Phone numbers (or those issued by Zoom's underlying service providers to Zoom Phone customers). To date, Zoom has not received any requests for traceback assistance from the Industry Traceback Group (ITG). However, Zoom will cooperate with the ITG, the FCC and state agencies charged with investigating the origins of illegal robocalls. Zoom has also committed contractually with its underlying service providers to participate in their traceback efforts and engages with these carriers regularly to investigate suspicious usage.

Zoom has designated a team for Fraud monitoring as the dedicated point of contact for addressing requests from other service providers or the ITG related to suspicious or illegal traffic. As a back-up, the Zoom Trust and Safety Team may also address such requests.

Zoom will respond to requests promptly (within 4 business hours) and will make commercially reasonable efforts to ensure that results are returned within 24 hours.

FCC CERTIFICATION

On June 25, 2021, Zoom Voice Communications Inc. certified with the FCC that its network is fully compliant with the STIR/SHAKEN framework.

POINTS OF CONTACT

TRACEBACK REQUESTS (Main Contact)	TRACEBACK REQUESTS (Backup Contact)	FCC CERTIFICATION AND RELATED LEGAL MATTERS
Fraud Team for Traceback	Fraud Team	Lynn Haaland Deputy General Counsel
traceback@zoom.us (888) 799-9666 (U.S. Business Hours, Pacific Time)	anti-fraud@zoom.us (888) 799-9666 (U.S. Business Hours, Pacific Time)	zp-compliance@zoom.us (888) 799-9666 (U.S. Business Hours, Pacific Time)

RECORDKEEPING

Zoom keeps records of all complaints it receives from customers concerning robocalls originated on its network. To the extent that Zoom receives traceback requests, Zoom will retain information related to the request for a period of two years from receipt.

ONGOING COMPLIANCE AND REEVALUATION

There are several stakeholders at Zoom involved in ensuring that Zoom develops and maintains organizational measures designed to mitigate illegal robocalls and spoofing on the Zoom Phone service.

Multiple internal teams across the company work together, including the Trust and Safety Team, Carrier Operations, Product Team, and the Fraud Team stakeholders, across Zoom to ensure that policies and procedures meet Zoom's legal obligations with respect to robocall mitigation. Zoom also may conduct training and develop checklists, as necessary, to ensure that all internal stakeholders understand Zoom's legal obligations. To the extent that revisions to the Robocall Mitigation Program are necessary to keep pace with changes in Zoom's business arrangements, services, increased threat of robocalling or other developments, Zoom will conduct a gap analysis and revise the Robocall Mitigation Plan accordingly. To the extent that a significant or systemic failure occurs with respect to Zoom's robocall mitigation measures, Zoom will draft an incident report to document such failure and provide a root cause analysis. The report will include a summary of acts Zoom has taken to remediate the incident.
