



ROBOCALL MITIGATION PROGRAM

Zoom Online Group LLC & affiliates (“Zoom Online”)

This Robocall Mitigation Program (RMP) describes with particularity the steps Zoom Online takes to avoid the origination, carrying, or processing of illegal robocall traffic. Zoom Online is a United States-based company offering a suite of fiber-based services, including high speed broadband Internet access and voice services to retail business and residential customers. Zoom Online does *not* originate wholesale or international traffic, and is *not* an intermediate provider or gateway provider. Zoom Online does *not* originate telemarketing, high-volume, short-duration, or auto-dialer traffic. Zoom Online does *not* receive intermediate traffic from upstream providers. Zoom Online has *not* been prohibited from filing in the Robocall Mitigation Database pursuant to law enforcement action. This RMP will be updated as regulations and business practices evolve.

Tracebacks/Law Enforcement Inquiries

Zoom Online commits to respond within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. Zoom Online’s contact for tracebacks/law enforcement inquiries (and employee responsible for addressing robocall mitigation issues) is:

- Contact Name: Wayne D’sa
- Phone: (602) 576-5150
- Email: wayne@zoomonline.com cc: pphipps@qsiconsulting.com
- Address: 500 N. Akard
Ross Towers, Suite 3475
Dallas, TX 75201

Call Analytics

Zoom Online monitors and analyzes voice traffic originated on its network, and utilizes call analytics systems to identify and block illegal traffic. Traffic is analyzed to identify high-volume, short-duration, or other traffic patterns indicative of robocalling campaigns.

Zoom Online uses third-party vendor TransNexus’s ClearIP platform, which provides a portfolio of tools enabling analytics, telecom fraud prevention, robocall prevention, and STIR/SHAKEN caller ID authentication and verification. ClearIP provides analytics that can be reviewed according to the following call attributes: customer, provider, trunk, subscriber, IP address and telephone number. ClearIP analyzes voice traffic and performs dynamic fraud analysis to detect and prevent fraud attacks. Fraud prevention actions include: automatic blocking, call teardown, notification. Fraud prevention also includes the capability to blacklist/whitelist by telephone number, SPID/OCN, IP address, etc. ClearIP also prevents unwanted robocalls and Denial of Service (DoD) attacks via real-time traffic analysis, blocking, etc.



Zoom Online investigates suspicious call patterns. If a pattern consistent with illegal robocalls or other fraudulent traffic is identified, Zoom Online will identify the party that is using its network in such manner and take appropriate action to stop processing the traffic. Appropriate action may include suspension of service, blocking, or notifying law enforcement.

Acceptable Use Policy

Zoom Online voice service customers must adhere to the company's Acceptable Use Policy (AUP), available at the following link: <https://zoomonline.com/wp-content/uploads/2024/01/ZoomOnline-Acceptable-Use-Policy.pdf>. Zoom Online's AUP identifies illegal robocalling and other fraudulent traffic as a prohibited use of the company's service, and authorizes the company to take immediate action including service suspension and termination (with or without written notice) to address such traffic.

STIR/SHAKEN Implementation

Zoom Online has implemented STIR/SHAKEN (S/S) caller ID authentication and verification via third-party vendor TransNexus's ClearIP platform. Calls originated by Zoom Online will be signed with a S/S token reflecting Zoom Online's credentials.

Know-Your-Customer

Zoom Online performs due diligence to know its customers and takes affirmative measures to prevent new and renewing customers from originating illegal calls.

During customer onboarding, Zoom Online collects specific information about its customers to ensure their legitimacy via a service application process. That information includes: Contact Person, Address details, Contact email, telephone number, and Credit Card. Zoom Online checks this information as part of our Customer Verification Process. When a customer renews service or adds service, Zoom Online request's the customer to accept the terms only for the new service which is added.

When Zoom Online customers enter into a contract for voice service, that contract incorporates by reference the company's Acceptable Use Policy that addresses the identification and resolution of illegal/fraudulent voice traffic.

Customer Education

Zoom Online posts information on its website to educate customers on how to protect themselves from becoming a victim of unlawful robocalls and a process to report complaints related to robocall activity. This can be viewed under the FAQ link on the ZoomOnline were here at: <https://zoomonline.com/faq>