

Zoom Networks Robocall Mitigation Program

1. Introduction

Zoom Networks, a provider of IP -based telecommunication services, is committed to the highest standards of lawful and ethical practices. This document outlines our comprehensive Robocall Mitigation Program, designed to prevent the origination of illegal robocall traffic.

2. Infrastructure and Management

Our PBX infrastructure is hosted on our internal datacenter hardware, utilizing an IPbased system. This setup is managed by our dedicated internal team, ensuring regular quality and security updates. We employ rigorous monitoring for irregular activity, unauthorized access, or anomalies indicating malicious or illegal activity, primarily using SIP-based communication protocols.

3. Deployment of Endpoints and Autodialers

Client requests for new endpoints or autodialers are meticulously processed. We collect detailed information on location, user, and intended purpose. Each request undergoes a strict compliance review, with uncompliant requests being immediately rejected.

Accepted requests are incorporated into the customer's PBX with necessary compliance measures, such as E -911 location information. All equipment is pre -configured and sent to clients, who do not possess reprogramming capabilities.

4. Monitoring and Analysis

Our monitoring involves weekly analysis of call logs to identify deviations from normal traffic patterns. Special attention is given to international calls, which are flagged for immediate review. Automated alerts are set up to notify us of unusual IP origination or activity from known bad actors. We also conduct random call recording reviews and analyze outgoing call patterns, frequency, and durations to detect unauthorized usage or dialing campaigns.

5. End-User Verification

We enforce strict verification processes for our clients. This includes obtaining business registrations, conducting reputational checks via public sources, and establishing direct communication with company administrators. These checks are performed initially and on an annual basis to maintain the authenticity and validity of our client base.

5a. Know Your Customer (KYC) Plan

Zoom Networks' Know Your Customer (KYC) process is integrated directly into our client engagement model. Because our services are not offered through open or anonymous sales channels, all customers are existing or referred clients of our IT support services and are personally vetted by our staff.

- Direct Vetting: Each customer relationship is established through direct interaction, including confirmation of business operations, administrative contacts, and service requirements.
- No Third-Party Vendor Use: Zoom Networks does not employ third-party vendors for KYC analytics. All verifications and reviews are conducted internally by our compliance and support staff.
- Ongoing Assurance: As part of our IT support relationships, client legitimacy and operational integrity are continuously monitored. Any irregularities identified during routine service interactions or annual reviews result in immediate investigation and, if necessary, escalation under our Robocall Mitigation Program.

This process ensures that all clients are known, legitimate entities and eliminates the risk associated with anonymous or unverified accounts.

6. Employee Training and Awareness

Employees are trained on both sandbox and live systems to distinguish between legitimate and suspicious call patterns. Training is conducted one -on-one for

maximum retention. Ongoing accuracy is ensured through quarterly reviews where randomly selected investigations are cross-checked by a different team member. Any anomalies result in intensified supervision and review until satisfactory performance is reestablished.

7. Incident Response and Reporting

In the event of a suspected illegal robocall incident, a two-step verification process is initiated. Confirmed incidents lead to immediate account suspension and issuance of a notice to the involved party. If the response is inadequate or absent within a 7-day period, the account is terminated, and the service is blacklisted. Such incidents are reported to the FCC following this period or upon confirmation of malicious traffic.

8. Technology Solutions

Our current systems are predominantly manual. However, we have implemented the STIR/SHAKEN technology to enhance our capabilities in detecting and preventing robocalls.

9. Review and Audit

Our strategies and controls are reviewed annually or in response to significant shifts in national robocall patterns or regulatory changes. These reviews are conducted by our administrative staff, with findings directly influencing company policies, technological frameworks, and employee training programs.

10. Conclusion

At Zoom Networks, we stand firmly against illegal robocalling activities and are dedicated to upholding the integrity of telecommunications. Through our robust Robocall Mitigation Program, we pledge to maintain compliance with all relevant regulations and to continuously improve our practices for the benefit of our clients and the wider community.