

Robocall Mitigation Plan for Mobile PC Guys, LLC (DBA Lifeline Voice & Data)

1. Business Overview

We are a small company that provides voice communication services to small businesses and government offices with less than 100,000 voice service subscriber lines. We are a reseller of voice services, relying on our upstream Voice Service Provider for call routing and STIR/SHAKEN implementation.

We do not provide any SIP trunking. We specifically deny service to any call centers, political campaign callers, fund raising centers or other bulk calling businesses or agencies. We are a hosted PBX provider, where our customers have IP phones connected to our hosted phone system. Because of this, it is not possible for a customer to use any sort of robo-call generation system, power dialer, etc. to generate calls. In addition, our IP phone system has integrated fraud control software (because it is capable of handling sip trunking, although we do not provide this service). This system is set to disable any account generating heavy outbound traffic.

We have designed our call management platform to restrict any form of autodialing, predictive dialing, or prerecorded message functionalities, allowing only manual outbound calls initiated by human users.

This plan outlines our measures to comply with FCC requirements under 47 CFR § 64.6305(a) and highlights our system's inherent restrictions, which actively prevent the origination of illegal robocalls.

2. System Safeguards to Prevent Illegal Robocalls

Our platform is configured to eliminate the possibility of originating illegal robocalls

through the following enforced measures:

A. Manual Dialing Only:

- o All outbound calls must be manually initiated by human users.
- o Autodialing, predictive dialing, and prerecorded message functionalities are permanently restricted and disabled from our customer's access.

B. Caller ID Integrity:

- o Caller ID spoofing is prohibited by default through system-level controls.
- o Only verified and authorized caller IDs are permitted and entered by our team.

These safeguards ensure that illegal robocalls cannot originate through our services, reducing the need for extensive monitoring of restricted activities.

3. Customer Vetting and Onboarding

To prevent misuse of our services, we conduct thorough vetting during the onboarding process.

A. Customer Information Collection

Before onboarding, we collect and verify the following details from all prospective customers:

- Legal business name and physical address.
- Nature of the customer's business and intended use of our services.

B. Ongoing Customer Oversight

Even after onboarding, we continue to monitor general traffic patterns to ensure usage aligns with the customer's stated business purpose.

4. Proactive Monitoring and Analysis

While our system inherently prevents illegal robocalls, we employ the following measures to ensure ongoing compliance and detect any potential misuse:

1. Customer Activity Oversight:

- o We review general traffic patterns to confirm that usage aligns with the customer's stated business purpose.
- o Unusual traffic trends, such as unexpected spikes in call volumes or destination anomalies, are flagged for review.

2. Enforcement Actions:

- o If any suspicious activity is identified, services are suspended pending investigation.
- o Violations result in immediate account termination and notification to relevant authorities.

These monitoring efforts, while minimal due to our system's restrictions, demonstrate our continued commitment to ensuring compliance.

5. Traceback Cooperation

We are fully committed to cooperating with traceback requests within 24 hours, as required by the FCC. To support this commitment, we:

1. Maintain accurate and detailed call records for all traffic originating through our system.
2. Promptly respond to inquiries from the FCC, Industry Traceback Group (ITG), and law enforcement.
3. Implement corrective actions, such as blocking traffic or terminating accounts, when violations are identified.

6. Enforcement and Call Blocking

Our policies are enforced through the following measures:

1. **Proactive Blocking:** Any suspicious or verified illegal traffic is blocked immediately.
2. **Account Termination:** Customers found in violation of our policies face immediate account termination.
3. **Post-Incident Reviews:** All incidents are reviewed to improve processes and prevent recurrence.

7. Contact Information

For questions regarding this Robocall Mitigation Plan, please contact:

Mobile PC Guys, LLC

DBA Lifeline Voice & Data

731-588-4200

wendy@lifelinevoice.com