

Robocall Mitigation Plan

PBX SIP Trunking LLC

Date: October 13, 2024

1. Introduction

PBX SIP Trunking LLC is committed to providing secure and reliable telecommunications services to our customers. As part of our dedication to maintaining high-quality service and adhering to regulatory standards, we have developed this Robocall Mitigation Plan. This plan outlines the strategies, technologies, and procedures we employ to prevent, detect, and mitigate unauthorized robocalls within our network.

2. Objectives

- **Prevent Unauthorized Robocalls:** Implement measures to block and reduce the incidence of unsolicited automated calls.
- **Protect Consumers:** Safeguard our customers from fraudulent and nuisance calls that may compromise their privacy and security.
- **Ensure Regulatory Compliance:** Adhere to all Federal Communications Commission (FCC) regulations and guidelines related to robocall prevention.
- **Enhance Network Integrity:** Maintain the reliability and trustworthiness of our telecommunications services by minimizing robocall-related disruptions.

3. Current Status

As a newly established company, PBX SIP Trunking LLC is in the process of building its telecommunications infrastructure. While we have not yet implemented the STIR/SHAKEN protocols, we recognize their importance in combating caller ID spoofing and are actively planning their integration into our network. In the interim, we have adopted a multi-faceted approach to mitigate robocalls through existing technologies and best practices.

4. Robocall Mitigation Strategies

Our comprehensive mitigation strategy encompasses the following key areas:

4.1 Caller Authentication

- **Caller ID Verification:** Implement systems to verify the authenticity of incoming caller IDs, reducing the likelihood of spoofed numbers.
- **Authentication Protocols:** Utilize industry-standard authentication protocols to ensure that calls originate from legitimate sources.

4.2 Call Filtering and Blocking

- **Automated Filtering:** Deploy automated systems to detect and block known robocall patterns and sources.
- **Blacklist Management:** Maintain and regularly update blacklists of known spam and fraudulent numbers to prevent their access to our network.
- **Whitelist Implementation:** Encourage customers to use whitelists for trusted contacts, minimizing the impact of unwanted calls.

4.3 User Reporting and Feedback

- **Reporting Mechanism:** Provide customers with easy-to-use tools to report suspected robocalls, enabling us to identify and address new threats promptly.
- **Feedback Integration:** Incorporate user feedback into our filtering algorithms to enhance the accuracy and effectiveness of our mitigation efforts.

4.4 Rate Limiting and Throttling

- **Call Rate Limits:** Implement rate limiting to control the number of calls that can be initiated from a single source within a specified timeframe.
- **Throttling Mechanisms:** Apply throttling techniques to slow down call attempts from suspicious sources, discouraging large-scale robocall campaigns.

5. Technical Measures

5.1 Advanced Call Analytics

- **Machine Learning Models:** Utilize machine learning algorithms to analyze call patterns and identify potential robocalls based on behavioral indicators.
- **Real-Time Monitoring:** Implement real-time monitoring systems to detect and respond to robocall activities as they occur.

5.2 Network Security Enhancements

- **Secure Infrastructure:** Ensure that our telecommunications infrastructure is fortified against unauthorized access and exploitation.
- **Encryption:** Use encryption technologies to protect call data from interception and tampering.

5.3 Integration with Third-Party Solutions

- **Partnerships:** Collaborate with third-party robocall detection and prevention service providers to leverage their expertise and advanced technologies.
- **API Integration:** Integrate third-party APIs to enhance our call filtering and authentication capabilities.

6. Procedural Measures

6.1 Policy Development

- **Robocall Policy:** Establish and enforce internal policies governing the prevention and handling of robocalls within our network.
- **Employee Training:** Conduct regular training sessions for employees to ensure awareness and adherence to robocall mitigation policies.

6.2 Incident Response Plan

- **Detection and Identification:** Develop procedures for the timely detection and identification of robocall incidents.
- **Containment and Mitigation:** Outline steps to contain and mitigate the impact of detected robocalls, including blocking offending numbers and informing affected customers.
- **Post-Incident Review:** Perform thorough reviews of robocall incidents to identify root causes and implement corrective actions.

6.3 Compliance and Reporting

- **Regulatory Compliance:** Ensure all mitigation measures align with FCC regulations and guidelines.
- **Reporting Obligations:** Fulfill all required reporting obligations to the FCC, including data on robocall incidents and mitigation efforts.

7. Compliance with FCC Guidelines

PBX SIP Trunking LLC adheres to the following FCC regulations and guidelines to ensure effective robocall mitigation:

- **Telephone Consumer Protection Act (TCPA):** Comply with TCPA provisions regarding automated calls and caller identification.
- **Robocall Mitigation Rules:** Implement FCC-recommended best practices for preventing and addressing robocalls.
- **STIR/SHAKEN Framework Preparation:** Although not yet implemented, design our systems to facilitate future compliance with STIR/SHAKEN protocols.

8. Implementation Plan

Phase	Activities	Timeline
Planning	Define requirements, select mitigation technologies	Months 1-2
Design	Develop system architecture and integration plans	Months 3-4
Development	Build and configure call filtering and authentication systems	Months 5-6
Testing	Conduct functionality, security, and performance testing	Months 7-8
Deployment	Launch robocall mitigation systems in the production environment	Month 9
Training and Documentation	Train staff and create comprehensive procedural documentation	Month 9
Maintenance and Review	Ongoing support, updates, and periodic reviews	Ongoing

9. Monitoring and Reporting

9.1 Continuous Monitoring

- **Real-Time Surveillance:** Implement continuous monitoring tools to track call activities and identify anomalies indicative of robocall campaigns.
- **Alert Systems:** Set up automated alerts to notify relevant personnel of potential robocall incidents for immediate action.

9.2 Reporting Mechanisms

- **Internal Reporting:** Generate regular internal reports detailing robocall metrics, mitigation effectiveness, and areas for improvement.
- **FCC Reporting:** Submit required reports to the FCC, including data on robocall incidents, mitigation measures taken, and compliance status.

10. Future Enhancements

10.1 STIR/SHAKEN Implementation

- **Planning and Integration:** Develop a roadmap for integrating STIR/SHAKEN protocols into our network to enhance caller authentication and reduce spoofing.
- **Testing and Deployment:** Conduct thorough testing of STIR/SHAKEN components before full-scale deployment to ensure seamless integration and compliance.

10.2 Enhanced Machine Learning Models

- **Algorithm Improvement:** Continuously refine machine learning models to improve the accuracy of robocall detection and reduce false positives.

- **Data Enrichment:** Incorporate additional data sources and contextual information to enhance the decision-making capabilities of our analytics systems.

10.3 Customer Education Programs

- **Awareness Campaigns:** Launch initiatives to educate customers about robocalls, including how to recognize and report suspicious activities.
- **Support Resources:** Provide comprehensive support resources, such as FAQs and guides, to help customers manage and mitigate robocalls effectively.

11. Conclusion

PBX SIP Trunking LLC is dedicated to combating robocalls and protecting our customers from unwanted and fraudulent communications. Through a combination of advanced technologies, robust procedures, and a commitment to regulatory compliance, we strive to minimize the impact of robocalls on our network and ensure a secure telecommunications environment. As we continue to grow, we will enhance our mitigation strategies, including the implementation of STIR/SHAKEN protocols, to stay ahead of evolving robocall threats.