

Robocall Mitigation Program for

Executive Summary

This document outlines the Robocall Mitigation Program for Zenith VoIP LLC designed to comply with the Federal Communications Commission (FCC) requirements, specifically 47 CFR § 64.6305(a). The program aims to protect consumers from illegal robocalls and ensure the integrity of the telecommunications network.

Introduction

Robocalls have become a significant concern for consumers, regulators, and telecommunications providers. The FCC has established strict guidelines to mitigate the impact of illegal and unwanted robocalls. Zenith VoIP LLC is committed to adhering to these guidelines, including the requirements of 47 CFR § 64.6305(a), to protect our customers and the broader telecommunications ecosystem.

Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium within 24 hours of traceback being received, and cooperate with such entities in investigating and stopping any illegal Robocalls that use our service to originate calls.

Program Objectives

1. ****Prevent Illegal Robocalls****: Implement measures to identify and block illegal robocalls before they reach consumers.
2. ****Enhance Call Authentication****: Deploy STIR/SHAKEN protocols to verify the legitimacy of calls.
3. ****Collaboration and Reporting****: Work with industry stakeholders and regulatory bodies to share information and report violations.
4. ****Consumer Education and Protection****: Inform customers about robocall mitigation efforts and provide tools to help them manage unwanted calls.

Program Components

1. Call Authentication and Verification

Zenith VoIP LLC will implement the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) protocols as mandated

by the FCC. These protocols will ensure that all calls transmitted over our network are authenticated, reducing the likelihood of spoofed calls.

Key Actions:

- **Deploy STIR/SHAKEN**: Integrate STIR/SHAKEN into our network infrastructure.
- **Monitor Call Traffic**: Continuously monitor call traffic for signs of spoofing or other malicious activities.
- **Caller ID Authentication**: Ensure that all outbound calls have valid caller ID information.

2. Robocall Detection and Blocking

We will implement advanced analytics and machine learning algorithms to detect and block illegal robocalls. These tools will analyze call patterns and behaviors to identify and mitigate potential threats.

Key Actions:

- **Real-Time Analytics**: Use real-time analytics to detect suspicious call patterns.
- **Blacklist and Whitelist Management**: Maintain and update lists of known robocall sources and legitimate callers.
- **Automated Blocking**: Automatically block calls identified as illegal robocalls based on our detection algorithms.

3. Consumer Education and Support

Educating our customers about robocalls and providing them with tools to manage unwanted calls is crucial for the success of our program. We will offer resources and support to help consumers protect themselves.

Key Actions:

- **Educational Campaigns**: Launch campaigns to inform customers about robocall risks and mitigation strategies.
- **Support Channels**: Provide dedicated support channels for customers to report robocalls and seek assistance.
- **Robocall Mitigation Tools**: Offer tools such as call blocking and filtering services to help consumers manage incoming calls.

4. Regulatory Compliance and Reporting

Zenith VoIP LLC will ensure full compliance with all FCC regulations regarding robocall mitigation, particularly 47 CFR § 64.6305(a). We will also participate in industry forums and report any violations to the appropriate authorities.

Key Actions:

- **Compliance Audits**: Conduct regular audits to ensure compliance with FCC requirements.
- **Industry Collaboration**: Engage with industry stakeholders to share best practices and collaborate on mitigation efforts.
- **Violation Reporting**: Report any detected violations to the FCC and other relevant authorities.

Implementation Timeline

Phase 1: Planning and Assessment (Months 1-3)

- Assess current infrastructure and capabilities.
- Develop a detailed implementation plan.
- Begin stakeholder engagement and collaboration efforts.

Phase 2: Deployment and Integration (Months 4-6)

- Deploy STIR/SHAKEN protocols.
- Integrate detection and blocking systems.
- Launch initial consumer education campaigns.

Phase 3: Monitoring and Optimization (Months 7-12)

- Monitor system performance and effectiveness.
- Optimize detection algorithms and blocking mechanisms.
- Continue consumer education efforts and support.

Phase 4: Ongoing Compliance and Improvement (Ongoing)

- Conduct regular compliance audits.
- Update systems and protocols based on emerging threats and regulatory changes.
- Maintain open communication channels with industry stakeholders and regulators.

Conclusion

Zenith VoIP LLC is committed to protecting our customers from illegal robocalls and ensuring the integrity of our telecommunications network. By implementing this Robocall Mitigation Program, we aim to comply with FCC requirements, specifically 47 CFR § 64.6305(a), and contribute to the broader effort to combat robocalls. Our approach combines advanced technology, consumer education, and regulatory compliance to create a safer and more secure communication environment.

This paper provides a comprehensive framework for Infinityconnect LLC's Robocall Mitigation Program, aligning with FCC requirements and demonstrating our commitment to combating illegal robocalls