

iTekz, LLC recognizes the critical importance of combating illegal and fraudulent robocalls to protect consumers and maintain the integrity of voice communication networks. Our **Robocall Mitigation Program** is a proactive, comprehensive initiative designed to meet and exceed FCC requirements, including adherence to STIR/SHAKEN protocols and other industry best practices.

This document outlines our program's framework, compliance measures, and ongoing commitment to mitigating the impact of unlawful robocalls.

Program Overview

1. Objective

To identify, mitigate, and prevent illegal robocall traffic originating from or traversing our network, while maintaining compliance with FCC regulations and promoting trust in telecommunications.

2. Scope

- Apply to all voice traffic, including IP-based and TDM systems.
- Ensure collaboration with downstream and upstream providers for end-to-end mitigation.
- Educate customers and stakeholders about robocall risks and prevention measures.

Mitigation Framework

1. Call Authentication (STIR/SHAKEN)

- Full implementation of STIR/SHAKEN protocols for IP-based voice traffic to authenticate caller IDs and prevent spoofing. Utilizing only vendors, such as Bandwidth, who fully comply with this regulatory standard.
- Collaborate with carriers to extend authentication to non-IP traffic where technically feasible.
- Certify compliance with STIR/SHAKEN in the Robocall Mitigation Database.

2. Network Monitoring and Analysis

- Deploy advanced analytics to monitor call patterns and detect anomalies indicative of robocall activity.
- Utilize AI-driven tools to identify and flag potential illegal robocalls in real time.
- Maintain detailed records of flagged, blocked, or allowed calls for auditing and reporting purposes.

3. Proactive Blocking Measures

- Implement call-blocking mechanisms to prevent known illegal or high-risk calls from reaching end-users.
- Regularly update blacklists using data from trusted industry sources and regulatory agencies.
- Test and refine blocking technologies to minimize false positives and ensure legitimate calls are unaffected.

4. Reporting and Compliance

- Submit required reports to the FCC, detailing our robocall mitigation efforts and compliance progress.
- Maintain and update our Robocall Mitigation Database registration, providing transparency about our measures.
- Respond promptly to inquiries or complaints from the FCC and other regulatory bodies.

5. Customer Education and Support

- Provide educational materials to customers about robocall risks, prevention, and reporting.
- Offer tools such as call-blocking apps or account settings to help users manage unwanted calls.
- Establish a dedicated support team to address customer concerns related to robocalls.

Conclusion

iTekz, LLC is fully committed to protecting consumers and maintaining compliance with FCC regulations through a robust and adaptive Robocall Mitigation Program. We will continue to monitor, update, and refine our strategies to stay ahead of evolving threats and provide secure, reliable communication services.

For further details or inquiries, please contact:

Pablo Rivas
pdr@itekz.com

Submitted by:

Pablo Rivas