

Robocall Mitigation Plan for Telin Systems

1. Purpose of the Plan

Telin Systems is committed to complying with the Federal Communications Commission (FCC) robocall mitigation requirements and ensuring the integrity of our voice communications services. This plan outlines the measures we take to prevent and mitigate unlawful robocalls using our systems.

2. Compliance with Twilio's Robocall Mitigation Tactics

Telin Systems fully adheres to Twilio's established robocall mitigation best practices, including:

- Implementation of Twilio's **STIR/SHAKEN protocol** to authenticate and verify caller identities.
- Monitoring and enforcement of usage policies to detect and prevent suspicious call traffic patterns.
- Proactive use of Twilio's **Voice Insights and Fraud Detection** tools to identify potential robocall traffic.
- Compliance with Twilio's **Know Your Customer (KYC)** guidelines to ensure legitimate use of the platform by our customers.

3. Customer Access Controls

Telin Systems does not grant customers direct access to Twilio's platform for configuration or modification of services. All Twilio-related system adjustments, configurations, and updates are managed exclusively by Telin Systems' trained technical team. This ensures that no unforeseen or unauthorized changes can be made by customers, further reducing the risk of abuse.

4. Monitoring and Traffic Analysis

Telin Systems maintains comprehensive monitoring of call traffic to identify unusual patterns indicative of unlawful robocall activity. Any suspicious activity is promptly investigated and addressed. This includes leveraging Twilio's real-time analytics tools to:

- Identify spikes in call volume from specific accounts.
- Detect and block high-risk call destinations.
- Analyze call duration, frequency, and geographic distribution to flag potential misuse.

5. Customer Vetting and Ongoing Evaluation

Telin Systems enforces strict vetting procedures for all customers to ensure lawful and compliant usage of our voice services. This includes:

- Verifying customer identity and intent during onboarding.
- Periodic reevaluation of customer usage patterns to ensure continued compliance.
- Immediate suspension or termination of service for customers found engaging in unlawful or unauthorized activity.

6. Response to Identified Robocall Activity

In the event unlawful robocall activity is detected, Telin Systems will:

1. Immediately suspend the affected account to prevent further abuse.
2. Conduct an internal investigation to determine the cause and scope of the activity.
3. Notify relevant authorities, including the FCC, as required.
4. Collaborate with Twilio to mitigate the impact of the detected robocalls.

7. Employee Training

All Telin Systems employees involved in the operation and management of voice communications services receive training on robocall mitigation techniques, Twilio's best practices, and regulatory compliance requirements.

8. Certification and Accountability

Telin Systems certifies compliance with the FCC robocall mitigation requirements and Twilio's policies. We are committed to ongoing evaluation and improvement of our mitigation efforts to protect the communications ecosystem.

Telins traffic is monitored and follows all items in accordance Appendix A as Twilio is our upstream and commercial partner.

Appendix A

[Robocall Mitigation Database Form - Robocall Mitigation Database](#)