

Robo-Mitigation Plan for Swift Link Telco

Update as of 01/01/2025

Executive Summary

This document outlines Swift Link Telco's robust and comprehensive strategy for mitigating unlawful robocalls. Located at 1317 Edgewater Dr, Suite 729, Orlando, FL 32804, Swift Link Telco is committed to compliance with FCC regulations, including maintaining an up-to-date certification in the Robocall Mitigation Database (RMD). The plan focuses on prevention, detection, response, and ongoing compliance.

Section 1: Prevention Strategies

1.1 Implementation of STIR/SHAKEN Protocols

- Swift Link Telco fully implements Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) frameworks.
- These protocols ensure caller ID authentication for calls traversing IP networks, reducing the risk of spoofed calls reaching end users.

1.2 Traffic Monitoring and Filtering

- Deploy advanced traffic analytics tools to monitor call patterns.
- Automatically block calls originating from known illegal robocall sources and suspicious international gateways.
- Maintain updated blocklists based on industry feedback and FCC advisories.
- 24HR MAXIMUM RESPONSE TIME FOR TRACEBACK and full cooperation with ITG.

1.3 Carrier-to-Carrier Agreements

- Establish clear, enforceable agreements with upstream and downstream carriers that mandate compliance with robocall mitigation practices.
- Require partners to provide evidence of adherence to STIR/SHAKEN and other mitigation measures.

1.4 Customer Education

- Provide tools and resources to help customers identify and report suspicious calls.
- Regularly update customers on measures they can take to protect themselves from robocalls.

Section 2: Detection and Mitigation Tools

2.1 Advanced Robocall Analytics Platforms

- Utilize machine learning algorithms to detect anomalies in call traffic.
- Identify patterns associated with high-volume illegal robocalls, such as short call durations and rapid-fire dialing.

2.2 Real-Time Call Screening

- Implement real-time call screening and flagging systems that analyze call behavior as calls are routed.
- Use caller ID reputation scoring to prioritize legitimate calls and block suspected robocalls.

2.3 Integration with Industry Databases

- Regularly synchronize with industry-shared databases of known illegal robocallers.
- Actively contribute to these databases by reporting confirmed robocall sources.

2.4 Spam Labeling Technology

- Partner with third-party labeling services to ensure end users are informed about potential spam calls.
- Provide opt-in options for customers to receive call labeling services.

Section 3: Response and Remediation

3.1 Complaint Handling and Escalation

- Establish a dedicated team to investigate robocall complaints received from customers, regulators, or industry peers.
- Escalate unresolved or critical issues to the Compliance Department for immediate action.

3.2 Collaboration with Authorities

- Maintain open communication channels with the FCC and other regulatory bodies.
- Share relevant data and findings promptly when requested.

3.3 Termination of Offending Traffic

- Swiftly terminate traffic from sources confirmed to be originating illegal robocalls.
- Notify the involved parties about the termination and offer guidance on compliance measures to reinstate traffic.

3.4 Continuous Feedback Loop

- Use customer feedback and analytics to refine mitigation strategies.
 - Regularly review and update internal policies to address emerging threats.
-

Section 4: Compliance and Reporting

4.1 Maintaining RMD Certification

- Ensure timely updates to the company's certification in the Robocall Mitigation Database.
- Address any deficiencies identified by the FCC promptly to avoid decertification.

4.2 Internal Audits and Training

- Conduct quarterly internal audits to evaluate the effectiveness of mitigation measures.
- Provide ongoing training to employees on robocall mitigation best practices and regulatory compliance.

4.3 Reporting Obligations

- Submit regular compliance reports to the FCC, detailing mitigation activities and outcomes.
- Notify the FCC immediately of significant security breaches or compliance issues.

4.4 Independent Verification

- Engage third-party auditors to verify adherence to robocall mitigation practices.
 - Share audit results with stakeholders to maintain transparency and trust.
-

Section 5: Future Enhancements

5.1 Adoption of Emerging Technologies

- Explore the use of artificial intelligence and blockchain technologies to further enhance call verification and fraud detection.

5.2 Expanded Collaboration

- Participate in industry forums and working groups focused on combating robocalls.
- Share insights and learnings to collectively improve mitigation strategies across the sector.

5.3 Customer-Centric Innovations

- Develop user-friendly mobile apps and web portals to empower customers to manage call blocking preferences and report robocalls.

Conclusion

Swift Link Telco remains steadfast in its commitment to mitigating unlawful robocalls and complying with all regulatory requirements. By leveraging cutting-edge technology, fostering industry partnerships, and maintaining transparency with regulators, the company aims to protect its customers and uphold the integrity of its services.