

D&P Digital Forensics LLC Robocall Mitigation Plan

Robocall Mitigation Plan

A Robocall Mitigation Plan outlines the steps an organization will take to reduce the number of robocalls and prevent fraudulent or illegal robocalls. This plan is critical for compliance with laws such as the TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence Act) and regulations set by the Federal Communications Commission (FCC). Below is a comprehensive plan designed to help mitigate robocall risks:

1. Establishing a Robocall Mitigation Team

Roles and Responsibilities:

Compliance Officer: Ensures the organization complies with FCC rules and industry best practices.

Technical Team: Manages the technology to prevent robocalls (e.g., call authentication systems).

Customer Support: Handles customer complaints related to robocalls and ensures timely resolutions.

Legal Team: Provides guidance on compliance with robocall regulations and reports illegal activities.

2. Implementing STIR/SHAKEN Protocol

What is STIR/SHAKEN:

A framework to authenticate calls and reduce spoofing (when the caller ID is falsified).

Actions Taken:

Deploy STIR/SHAKEN across all VoIP (Voice over Internet Protocol) networks.

Ensure the Caller ID information is accurate for outbound calls.

Regularly update and monitor STIR/SHAKEN systems for compliance.

3. Call Authentication and Call Blocking Tools

Call Authentication: Implement advanced tools for validating calls, including the STIR/SHAKEN system, as mentioned.

Blocking Technology:

Deploy robocall blocking solutions to screen incoming calls.

Implement features like call-tagging to identify potentially fraudulent calls.

4. Telemarketing Compliance Program (We do not sell VoIP Services to Telemarketing Companies)

Training: Regularly train telemarketing teams to adhere to Do Not Call (DNC) list regulations, including ensuring calls do not violate rules regarding time restrictions and frequency.

D&P Digital Forensics LLC Robocall Mitigation Plan

Call Monitoring: Continuously monitor outbound calls to ensure compliance with the rules for calling consumers and using opt-out language.

Verify Third-Party Callers: Ensure that all third-party vendors conducting marketing calls are compliant with applicable regulations (e.g., the National Do Not Call Registry).

5. Identifying and Reporting Fraudulent Calls

Fraud Detection:

Use AI-driven systems to detect suspicious call patterns that could indicate fraudulent activity.

Implement real-time alerts for unusual spikes in outbound or inbound robocalls.

Reporting:

Report suspected fraudulent robocall activity to the FCC and other appropriate regulatory bodies.

Encourage customers to report robocalls and provide a clear reporting mechanism.

6. Consumer Protection and Opt-Out Mechanisms

Opt-Out Features:

Ensure that all marketing calls provide a clear and easy method for consumers to opt out (e.g., "Press 1 to opt out").

Customer Education:

Provide educational resources for consumers about robocall risks, scams, and how to protect their information.

Develop a customer awareness program explaining the importance of blocking unknown or suspicious numbers.

7. Regular Audits and Reporting

Internal Audits: Conduct regular audits of outbound calling activities and technologies to ensure compliance with the plan.

External Audits: Hire third-party experts to assess compliance with robocall regulations and recommend improvements.

Documentation and Reporting:

Maintain records of all robocall mitigation activities and reports to demonstrate ongoing compliance.

Prepare quarterly or annual reports summarizing the number of robocalls identified, blocked, and prevented.

8. Collaborating with Industry Stakeholders

D&P Digital Forensics LLC Robocall Mitigation Plan

Partnering with Telecom Providers: Work closely with telephone service providers to ensure that industry-wide anti-robocall technologies like STIR/SHAKEN are implemented effectively.

Engagement with Regulatory Bodies: Maintain communication with the FCC, the Federal Trade Commission (FTC), and other relevant bodies to stay updated on new rules and best practices.

Participating in Industry Groups: Join industry groups such as the Robocall Mitigation Database and contribute to setting best practices for robocall reduction.

9. Legal Compliance and Enforcement

Compliance with the TRACED Act:

Ensure all calls are compliant with the TRACED Act, which mandates call authentication and provides penalties for illegal robocalling.

Penalties for Non-Compliance:

Establish clear internal policies regarding penalties for non-compliance or negligence in adhering to the robocall mitigation plan.

Ongoing Monitoring of Legal Changes:

Continuously monitor changes in robocall-related legislation and adjust the mitigation plan as needed.

10. Continuous Improvement

Feedback Loop:

Regularly solicit feedback from customers and stakeholders to improve call handling processes.

Technology Upgrades:

Invest in newer technologies and automated systems to enhance robocall detection, prevention, and customer experience.

Review and Update the Plan: Annually review and update the mitigation plan to incorporate new technologies, evolving regulations, and lessons learned from past experiences.

Conclusion:

Implementing a Robocall Mitigation Plan is essential for compliance with current laws, protecting consumers, and maintaining trust in communication systems. By deploying industry standards like STIR/SHAKEN, educating consumers, collaborating with industry partners, and regularly reviewing processes, an organization can significantly reduce the impact of robocalls and ensure a safer, more transparent calling environment.