

TELERINGS LLC

Robocall Mitigation Database (RMD) Plan

Introduction

Telerings is dedicated to adhering to the Federal Communications Commission's (FCC) guidelines regarding the prevention of illegal robocalls and ensuring consumer protection. This document outlines Telerings' Robocall Mitigation Database (RMD) plan, developed to align with the latest FCC regulations, including those set forth by the TRACED Act, and related rulings. Our goal is to mitigate robocalls, safeguard telecommunications networks, and foster consumer trust.

1. Compliance Overview

Telerings understands its responsibilities under the FCC's robocall mitigation rules and is committed to the following actions:

- **STIR/SHAKEN Implementation:** Guaranteeing caller ID authenticity for all IP-based voice calls to prevent spoofing.
 - **Mitigation for Non-IP Networks:** Introducing alternative call verification methods for non-IP systems.
 - **Robocall Mitigation Database Filing:** Submitting precise and detailed certifications to the FCC's RMD.
 - **Ongoing Call Monitoring and Blocking:** Vigilantly identifying and mitigating robocalls in real-time.
 - **Collaboration with Industry Groups:** Partnering with USTelecom's Traceback Group to trace and identify illegal robocall sources.
-

2. STIR/SHAKEN Deployment

Telerings has implemented the STIR/SHAKEN protocol across all IP-based voice networks, ensuring:

- **Caller ID Authentication:** Verifying the legitimacy of calls through cryptographic signatures.
 - **Seamless Integration:** Full compatibility with upstream and downstream service providers.
 - **Ongoing Monitoring:** Continuous monitoring of STIR/SHAKEN performance and immediate escalation of issues to the FCC.
 - **Fallback Procedures:** Retaining traceability for authenticated calls during transmission disruptions.
-

3. Robocall Mitigation for Non-IP Networks

For non-IP-based networks, Telerings has adopted the following mitigation strategies:

- **Network-Level Detection:** Analyzing call patterns in real-time to detect and block suspicious activity.
 - **Data Analytics:** Leveraging call detail records and pattern recognition to identify and address robocall threats.
 - **Fraud Management:** Utilizing advanced fraud detection tools to spot and investigate potential fraudulent calls.
 - **Continuous Review:** Regularly updating mitigation measures to address emerging threats in non-IP networks.
-

4. Robocall Mitigation Database Certification

Telerings' certification with the FCC includes:

- **Detailed Mitigation Practices:** A clear description of strategies implemented to identify, block, and mitigate robocalls, including STIR/SHAKEN and alternative measures.
 - **Point of Contact:** Providing a dedicated contact for FCC inquiries and traceback activities.
 - **Certification Integrity:** Ensuring all certifications are accurate, supported by internal audits, and compliant with FCC guidelines.
 - **Annual Updates:** Submitting updated certifications in line with FCC requirements or when substantial changes occur in mitigation practices.
-

5. Call Blocking Practices

To comply with FCC guidelines, Telerings employs the following call-blocking practices:

- **Blocklists for Known Robocallers:** Maintaining a regularly updated database of known illegal robocall sources.
 - **Real-Time Analytics:** Using AI-driven algorithms to identify and block suspicious calls with minimal false positives.
 - **Customer Protection:** Providing clear communication about blocked calls and ensuring a swift resolution process for any errors.
 - **Adaptive Blocking:** Continuously refining blocking techniques to balance efficiency and accuracy.
-

6. Collaboration with Industry Stakeholders

Telerings works closely with:

- **USTelecom Traceback Group:** Participating in traceback efforts to track and take action against illegal robocall sources.
 - **Telecom Providers:** Collaborating with other service providers to exchange best practices and bolster industry-wide efforts.
 - **Law Enforcement:** Assisting law enforcement in tracing and dismantling illegal robocall operations by providing technical insights and data.
-

7. Reporting and Recordkeeping

Telerings ensures full transparency and accountability in its mitigation efforts:

- **Call Logs:** Maintaining detailed logs of blocked or flagged calls, including associated metadata, to support traceback investigations.
 - **Traceback Documentation:** Recording all participation in traceback activities and the outcome of investigations.
 - **FCC Reporting:** Submitting timely and accurate reports to the FCC regarding mitigation efforts and responding promptly to inquiries.
 - **Compliance Audits:** Conducting internal audits to ensure all records are accurate and aligned with FCC requirements.
-

8. Customer Education and Support

Telerings is committed to empowering customers with the knowledge and tools to prevent robocalls:

- **Educational Resources:** Offering online resources, alerts, and materials to educate customers on recognizing and reporting robocalls.
 - **Dedicated Support:** Providing accessible customer support channels via phone, email, and online chat for robocall-related issues.
 - **Spam Call Alerts:** Offering tools for customers to receive alerts about spam calls and easily report or block them.
 - **Community Engagement:** Partnering with local organizations to raise awareness about robocalls and prevention methods.
-

9. Internal Governance

Telerings has established a dedicated team to ensure compliance and effective mitigation practices:

- **Policy Oversight:** Ensuring all policies adhere to FCC regulations and that mitigation efforts are executed properly.
- **Training Programs:** Regularly educating employees on the latest robocall mitigation policies and technologies.

- **Performance Reviews:** Continuously evaluating the effectiveness of mitigation strategies and making necessary improvements.
 - **Executive Reporting:** Providing periodic updates to senior management to ensure robocall mitigation remains a high priority.
-

10. Continuous Improvement

Telerings is committed to refining its robocall mitigation approach by:

- **Technological Advancements:** Exploring and implementing new technologies to counter evolving robocall tactics.
 - **Customer Feedback:** Incorporating feedback from customers and industry partners to refine mitigation strategies.
 - **Regulatory Monitoring:** Staying abreast of FCC rule changes and adjusting internal policies and practices accordingly.
 - **Research and Development:** Investing in R&D to create innovative solutions for preventing robocalls.
-

Conclusion

Telerings' Robocall Mitigation Database plan showcases our commitment to combating illegal robocalls and protecting consumers. By adhering to FCC guidelines and continuously improving our efforts, we aim to set a high standard in the telecommunications industry for robocall mitigation.