BRIZZLENET

Robocall Mitigation Database Plan

Introduction Brizzlenet is committed to full compliance with the Federal Communications Commission (FCC) rules regarding robocall mitigation and the prevention of illegal robocalls. This document outlines Brizzlenet's comprehensive Robocall Mitigation Database (RMD) plan, designed to meet all FCC requirements, protect consumers, and maintain the integrity of telecommunications networks. The plan addresses the latest FCC rules, including updates mandated by the TRACED Act and related rulings.

1. Compliance Overview Brizzlenet recognizes its obligations under the FCC's robocall mitigation rules, including:

- **Implementation of STIR/SHAKEN Framework**: Ensuring all IP-based voice calls originate with appropriate caller ID authentication.
- **Robocall Mitigation Program for Non-IP Networks**: Implementing alternative measures for call authentication and verification.
- **Robocall Mitigation Database Filing**: Submitting accurate and detailed certification to the FCC's RMD.
- **Call Blocking and Monitoring**: Actively identifying, monitoring, and mitigating illegal robocalls.
- **Partnership with USTelecom Traceback Group**: Participating in traceback activities to identify sources of illegal robocalls. **Respond to all traceback and complaints within 24 hours.**

2. STIR/SHAKEN Deployment Brizzlenet has deployed the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using Tokens (SHAKEN) protocols for all IP-based calls. This includes:

- **Caller ID Authentication**: Using cryptographic methods to verify the caller's identity and prevent spoofing.
- **Full Integration**: Ensuring compatibility with all upstream and downstream providers.
- **Monitoring and Reporting**: Regularly reviewing STIR/SHAKEN performance and reporting issues to the FCC.
- **Fallback Procedures**: Ensuring call delivery for authenticated calls that experience transmission issues while maintaining traceability.

3. Robocall Mitigation for Non-IP Networks Brizzlenet maintains non-IP-based systems and has implemented the following mitigation strategies:

- **Network-Level Filtering**: Detecting and blocking suspicious call patterns using real-time network analytics.
- **Call Detail Records Analysis**: Using data analytics and pattern recognition to identify illegal robocall traffic and improve the accuracy of mitigation actions.

- **Fraud Management Tools**: Employing third-party solutions and proprietary systems to flag and investigate suspect call activity.
- **Regular Updates**: Periodically reviewing and updating mitigation practices for non-IP traffic in line with emerging threats.

4. Robocall Mitigation Database Certification Brizzlenet’s FCC certification includes:

- **Description of Mitigation Practices**: Comprehensive details on how Brizzlenet identifies and blocks illegal robocalls, including STIR/SHAKEN implementation and alternative methods.
- **Contact Information**: Providing designated representatives for FCC inquiries and traceback activities, available during business hours.
- **Certification Accuracy**: Ensuring all statements in the filing are accurate, truthful, and backed by internal audits.
- **Annual Updates**: Filing updates to the certification as required by FCC rules, or sooner if there are significant changes to mitigation practices.

5. Call Blocking Practices To ensure compliance with FCC guidelines, Brizzlenet has implemented the following call blocking practices:

- **Blocking Known Illegal Numbers**: Utilizing a dynamic database of known illegal robocallers, updated regularly.
- **Real-Time Analytics**: Leveraging AI-driven tools and heuristic analysis to detect and block suspicious traffic with high accuracy.
- **Customer Protection Measures**: Providing transparency to customers, such as notifications for blocked calls, and ensuring swift resolution of mistaken call blocking incidents.
- **Adaptive Blocking Techniques**: Continuously refining algorithms to balance effective blocking with the minimization of false positives.

6. Collaboration with Industry Stakeholders Brizzlenet actively collaborates with:

- **USTelecom Traceback Group**: Participating in traceback activities to identify bad actors and implement solutions based on findings.
- **Other Providers**: Engaging in cooperative initiatives to share best practices and enhance overall industry mitigation efforts.
- **Law Enforcement Agencies**: Supporting investigations into illegal robocall operations by providing data, insights, and technical expertise.

7. Reporting and Recordkeeping Brizzlenet maintains detailed records of its robocall mitigation efforts, including:

- **Blocked Calls Logs**: Documenting all blocked and flagged calls with detailed metadata to facilitate traceback and investigations.
- **Traceback Activities**: Recording participation and findings in traceback investigations, including the volume of flagged traffic and resolved cases.
  Respond to all traceback and complaints within 24 hours as per FCC regulation.

- **FCC Reports**: Submitting periodic updates on mitigation efforts and responding to FCC inquiries promptly and accurately.
- **Compliance Audits**: Conducting internal audits to ensure all records are complete, accurate, and in line with FCC requirements.

8. Customer Education and Support Brizzlenet is dedicated to educating customers on robocall prevention:

- **Educational Materials**: Providing online resources, brochures, and alerts on how to identify and report robocalls effectively.
- **Support Channels**: Offering dedicated customer support through phone, email, and online chat to assist with robocall-related issues.
- **Spam Alert Features**: Enabling spam call alerts and providing tools for customers to block or report unwanted calls easily.
- **Community Outreach**: Partnering with local organizations to raise awareness about robocall scams and prevention methods.

9. Internal Governance Brizzlenet has established a dedicated compliance team responsible for:

- **Policy Oversight**: Ensuring the company's adherence to FCC rules and maintaining the integrity of its mitigation efforts.
- **Training Programs**: Developing comprehensive training programs to educate employees about robocall mitigation policies, tools, and procedures.
- **Performance Audits**: Conducting regular reviews of mitigation practices, evaluating their effectiveness, and making improvements where necessary.
- **Executive Reporting**: Providing periodic updates to executive leadership to ensure robocall mitigation remains a top corporate priority.

10. Continuous Improvement Brizzlenet is committed to enhancing its robocall mitigation efforts through:

- **Technological Advancements**: Evaluating and adopting new technologies to stay ahead of evolving robocall threats.
- **Feedback Mechanisms**: Using customer and industry feedback to refine mitigation strategies and improve overall effectiveness.
- **Regulatory Updates**: Actively monitoring FCC rule changes and adjusting policies and practices to maintain compliance.
- **Research and Development**: Investing in R&D to develop innovative solutions for combating robocalls.

Conclusion Brizzlenet's Robocall Mitigation Database plan demonstrates our commitment to combating illegal robocalls and protecting our customers. This comprehensive approach ensures compliance with FCC requirements and reinforces our role as a responsible telecommunications provider. By continuously improving our practices and collaborating with industry stakeholders, Brizzlenet aims to set a standard of excellence in robocall mitigation.