

Robocall Mitigation Program Description

Overview

Airtime Technologies Chile SPA is committed to combating illegal robocalls and ensuring the integrity of the telecommunications network. Our Robocall Mitigation Program is designed to identify, monitor, and prevent the origination of illegal robocalls in compliance with FCC regulations.

Key Components

1. Monitoring and Detection

- Traffic Analysis:
 - Implement real-time analysis of call traffic patterns to detect anomalies indicative of illegal robocalling activities.
 - Use advanced analytics and machine learning algorithms to identify suspicious calling behaviors.
- Blacklist and Whitelist Management:
 - Maintain and regularly update blacklists of known illegal robocallers and whitelists of legitimate callers.
 - Utilize industry-provided blacklists and contribute to shared resources to enhance detection capabilities.

2. Caller ID Authentication

- STIR/SHAKEN Implementation:
 - Implement the STIR/SHAKEN framework on all IP-enabled portions of our network.
 - Authenticate and verify caller ID information for calls originating on the compliant segment of the network, ensuring compliance with 47 CFR § 64.6301(a)(1) and (2).
- Non-IP Network Handling:
 - For non-IP network segments, apply alternative caller ID verification measures and participate in industry efforts to extend STIR/SHAKEN or equivalent frameworks to these segments.

3. Traceback and Cooperation

- Traceback Response:
 - Commit to responding fully and within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium.
 - Provide detailed call records and cooperate in the investigation and cessation of illegal robocall operations.

- Collaboration:
 - Work with other telecommunications providers, industry groups, and regulatory bodies to share information and best practices for robocall mitigation.

4. Customer and Staff Education

- Awareness Programs:
 - Conduct regular educational campaigns to inform customers about the dangers of illegal robocalls and how to avoid becoming victims.
 - Provide resources and tools for customers to report suspicious calls.
- Training:
 - Regularly train staff on the latest robocall mitigation techniques and compliance requirements.
 - Ensure employees are equipped to assist in the detection and prevention of illegal robocalls.

5. Policy and Compliance

- Internal Policies:
 - Develop and enforce internal policies to prevent the use of Airtime Technologies Chile spa's services for illegal robocalling.
 - Establish clear procedures for handling violations, including termination of services for confirmed illegal robocallers.
- Compliance Monitoring:
 - Regularly review and update the robocall mitigation program to ensure ongoing compliance with FCC regulations and industry standards.
 - Perform periodic audits and assessments to evaluate the effectiveness of the program and make necessary improvements.

Detailed Procedures

Call Traffic Monitoring

1. Data Collection:
 - Collect call detail records (CDRs) and other relevant data points from network equipment.
2. Pattern Analysis:
 - Analyze call patterns for high call volumes, short call durations, and repeated calls to sequential numbers.
 - Flag and investigate patterns that deviate from normal calling behavior.

Caller ID Authentication

1. STIR/SHAKEN Deployment:
 - Deploy STIR/SHAKEN across IP-enabled network segments.
 - Monitor call authentication results and take corrective actions for calls failing verification.

2. Non-IP Measures:

- Implement interim solutions for caller ID verification on non-IP segments.
- Participate in industry initiatives to develop non-IP caller ID authentication standards.

Traceback and Law Enforcement Cooperation

1. Traceback Protocol:

- Establish a dedicated team to handle traceback requests.
- Ensure rapid response and thorough investigation of traceback requests.

2. Data Sharing:

- Share relevant call data with industry traceback consortium and law enforcement agencies as required.

Education and Training

1. Customer Outreach:

- Provide educational materials via email, website, and social media.
- Offer tools for customers to report robocalls and block suspicious numbers.

2. Staff Training:

- Conduct regular training sessions on robocall mitigation practices and regulatory requirements.
- Update staff on new threats and mitigation technologies.

Policy Enforcement

1. Service Agreements:

- Include strict anti-robocall clauses in customer service agreements.
- Terminate services for customers found to be engaging in illegal robocall activities.

2. Compliance Checks:

- Perform routine compliance checks and audits.
- Implement corrective actions based on audit findings.