

PixelRiver Technology, LLC

1055 Stewart Ave, Bethpage, NY 11714

Robocall Mitigation Program Description

1. Purpose and Scope

This Robocall Mitigation Program outlines the measures and protocols implemented to prevent the origination, transmission, and termination of illegal robocalls on our network. It ensures compliance with FCC regulations, including **47 CFR § 64.6305**. The program applies to all traffic traversing our systems, including IP-based and non-IP-based traffic, for voice service providers, gateway providers, and nongateway intermediate providers.

2. Call Authentication Practices

- **STIR/SHAKEN Implementation (for IP-based traffic):**
 - All IP-based voice traffic originating on our network undergoes Secure Telephony Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using Tokens (SHAKEN) authentication.
 - Calls are signed with appropriate attestation levels (A, B, or C) depending on the validation of caller information.
 - Calls are verified upon receipt to ensure authenticity.
 - **Alternative Measures (for non-IP-based traffic):**
 - For non-IP traffic, we have implemented a robust robocall mitigation plan, including call traceback support and pattern analysis to identify and mitigate illegal robocalls.
-

3. Gateway Provider-Specific Measures

- **Ingress Traffic Monitoring:**
 - All inbound calls from foreign networks are subjected to stringent monitoring protocols to detect patterns associated with illegal robocalls.
 - Traffic is analyzed using advanced analytics and machine learning tools to identify high-risk call signatures.
- **Blocked/Flagged Call Handling:**
 - Any calls failing authentication or exhibiting illegal robocall characteristics are blocked or flagged for further investigation before termination.

4. Nongateway Intermediate Provider-Specific Measures

- **Intermediate Call Processing:**
 - We ensure that any calls passing through our network comply with FCC regulations and maintain appropriate authentication.
 - Calls lacking proper authentication tokens (e.g., STIR/SHAKEN) are either blocked or subjected to additional scrutiny.
- **Support for Traceback Efforts:**
 - We collaborate fully with traceback efforts initiated by the FCC, USTelecom, or other authorities to identify and eliminate the sources of illegal robocalls.

5. Call Monitoring and Analytics

- **Real-Time Call Traffic Monitoring:**
 - Implement real-time analytics tools to monitor call patterns and identify anomalies indicative of robocall activity.
 - Employ machine learning algorithms to enhance detection accuracy and reduce false positives.
- **Regular Reporting:**
 - Maintain records of flagged and blocked calls and generate periodic reports for internal review and regulatory compliance.

6. Call Traceback Collaboration

- Participate actively in industry traceback initiatives.
- Respond promptly to traceback requests from authorized entities to aid in identifying the origin of illegal robocalls.

7. Enforcement of Customer Accountability

- Enforce strict terms and conditions for customers and partners to prohibit the origination or facilitation of illegal robocalls.
- Take immediate action, including disconnection or account suspension, against violators.

8. Ongoing Updates and Compliance

- **Program Updates:**

- The robocall mitigation plan is reviewed and updated periodically to reflect technological advancements and regulatory changes.
 - **Training:**
 - Regularly train staff and partners on compliance requirements and best practices for identifying and mitigating illegal robocalls.
 - **Compliance Audits:**
 - Conduct internal audits to verify the effectiveness of the robocall mitigation measures and ensure continued compliance with FCC regulations.
-

Contact Information

Compliance Officer: John Killcommons

Contact Information: [noc @ pixelriver com] | [516 741 7960]

Address: 1055 Stewart Ave Bethpage, NY. 11714