

Pure CallerID: Robocall Mitigation Program Overview

Our Robocall Mitigation Program is designed to proactively detect, analyze, and prevent illegal and unwanted robocalling activities across our network. This program incorporates robust Know Your Customer (KYC) procedures, continuous real-time monitoring of call traffic—including calls per second metrics—and advanced machine learning algorithms to identify and block anomalous call patterns. Our comprehensive approach not only meets but exceeds FCC guidelines, ensuring compliance, transparency, and enhanced protection for consumers.

1. Program Objectives

- **Prevent and Mitigate Robocalls:**

Implement proactive measures to identify and block unauthorized or fraudulent call activities.

- **Enhance Consumer Trust:**

Ensure the integrity of our network by maintaining stringent security and identity verification practices.

- **Maintain Regulatory Compliance:**

Align our policies and operational procedures with FCC requirements and industry best practices.

- **Foster Continuous Improvement:**

Leverage advanced analytics and feedback mechanisms to continually refine our mitigation strategies.

2. Extensive Know Your Customer (KYC) Procedures

- **Customer Onboarding and Verification:**

- Require comprehensive identity documentation and verification during account setup.

- Employ multi-factor authentication processes to confirm customer identity.

- Integrate third-party data sources and identity verification services to cross-check and validate customer information.

- **Ongoing Monitoring and Review:**

- Periodically review and update customer profiles to reflect any changes in contact details or business operations.

- Monitor usage patterns to flag potential deviations that may indicate fraudulent activities.
- Enforce strict data retention and audit policies in line with privacy and regulatory requirements.

3. Real-Time Call Monitoring and Analysis

- **Call Traffic Metrics:**

- Continuously monitor key metrics such as calls per second (CPS) across the network.
- Implement thresholds and alerting systems to identify abnormal surges or patterns that could signify robocall campaigns.

- **Network Behavior Analysis:**

- Utilize real-time dashboards to visualize call flow, volume, and distribution across different geographic and demographic segments.
- Integrate automated systems that trigger in-depth analyses when unusual call patterns are detected.

4. Machine Learning and Advanced Analytics

- **Anomaly Detection Models:**

- Deploy machine learning algorithms that learn from historical call data to identify deviations from typical calling behaviors.
- Utilize clustering and pattern recognition techniques to discern potentially fraudulent call origination and termination patterns.

- **Predictive Analytics:**

- Leverage predictive models to forecast and mitigate emerging robocall trends.
- Continuously retrain models with updated data to ensure high accuracy and responsiveness to new tactics used by malicious actors.

- **Adaptive Response Systems:**

- Automate the classification of call events based on risk scores generated by machine learning models.

- Enable dynamic blocking or flagging of suspicious calls in real time, reducing reliance on manual interventions.

5. Incident Response and Escalation Procedures

• Traceback Requests:

- All traceback requests are processed and responded to within 24 hours.
- If a traceback identifies illegal or unwanted robocalling on the network, immediate escalation procedures are enacted to block traffic and suspend bad actors immediately.

• Alert and Notification Systems:

- Integrate automated alert systems that notify relevant operational teams when potential threats are detected.
- Maintain a dedicated incident response team trained to investigate and act upon suspicious call patterns.

• Escalation Protocols:

- Develop a structured escalation process for unresolved incidents, including immediate communication with regulatory authorities if necessary.
- Ensure that detailed logs and audit trails are maintained for all incidents to support post-event analysis and regulatory reporting.

6. Compliance, Audit, and Reporting

• Regulatory Adherence:

- Maintain comprehensive documentation of all mitigation efforts, including KYC verification, call monitoring data, and machine learning outputs.
- Regularly review and update policies to remain compliant with evolving FCC regulations and industry standards.

• Internal Audits and Third-Party Assessments:

- Conduct periodic internal audits and engage independent third-party evaluators to assess program efficacy and compliance.
- Implement corrective actions promptly based on audit findings to continuously improve the program.

- **Transparency and Reporting:**

- Generate detailed reports summarizing performance metrics, incident resolutions, and compliance measures.
- Provide regular updates to regulatory bodies and stakeholders as required by FCC guidelines.

7. Continuous Improvement and Training

- **Employee Training:**

- Provide ongoing training for staff involved in network monitoring, customer verification, and incident response to ensure they are updated on the latest tools and techniques.

- **Technology and Process Upgrades:**

- Invest in research and development to upgrade machine learning models and monitoring systems continuously.
- Collaborate with industry partners and regulatory bodies to share best practices and enhance overall network security.

Conclusion

Our Robocall Mitigation Program represents a comprehensive and dynamic approach to preventing illegal call activities. By integrating extensive KYC measures, real-time call monitoring, and state-of-the-art machine learning analytics, our program not only meets FCC regulatory requirements but also reinforces our commitment to consumer protection and network integrity. We continuously strive to innovate and improve our defenses against evolving robocall threats, ensuring that our mitigation efforts remain effective and forward-looking.