

Robocall Mitigation Plan

Introduction

As a Voice Service Provider (VSP), Smart Telecard Inc is committed to preventing the origination and transmission of illegal robocalls on our network. This Robocall Mitigation Plan (RMP) outlines the comprehensive measures we have implemented to comply with the Federal Communications Commission (FCC) regulations, including 47 C.F.R. §64.6305, and to protect consumers from unwanted and fraudulent calls. Our proactive approach includes call authentication, network monitoring, customer verification, and cooperation with regulatory and industry entities to ensure a secure communication environment.

STIR/SHAKEN Implementation

We have implemented STIR/SHAKEN protocols across the IP portions of our network to authenticate and verify caller identity. For calls originating on our network:

- **Full Attestation (A)** is applied to calls using telephone numbers assigned to our customers.
- **Partial Attestation (B)** is applied to numbers used for legitimate masking purposes but not directly assigned to us.

For non-IP portions of our network, we are actively evaluating solutions to implement call authentication protocols as industry standards and compatible technologies become available. We collaborate with our upstream providers, all of whom are registered in the Robocall Mitigation Database and have implemented STIR/SHAKEN, to ensure end-to-end call authentication.

Know Your Customer (KYC) Procedures

To prevent the misuse of our services for illegal robocalling, we have established robust KYC protocols for all new and renewing customers:

- **Identity Verification:** We collect and verify customer information, including business name, physical address, contact person(s), federal tax ID, state of incorporation, and the nature of the customer's business.
- **Website Validation:** Customers must provide a functional website, which we verify to ensure legitimacy.
- **Signed Agreements:** All customers sign a service agreement that explicitly prohibits the use of our services for illegal robocalling, spoofing, or other fraudulent activities.
- **Number Authentication:** We verify that customers have the right to use the telephone numbers associated with their accounts, cross-referencing with trusted databases and our softswitch logs.

Our Terms of Service (TOS) include strict prohibitions against:

- Providing deceptive or false caller ID information.
- Engaging in autodialing or unsolicited telemarketing.
- Violating local, state, federal, or industry regulations.
- Using our services for fraudulent activities.

Violation of these terms may result in immediate suspension or termination of service.

Network Monitoring and Analytics

We employ advanced call analytics and monitoring systems to detect and prevent illegal robocall traffic:

- **Real-Time Monitoring:** Our systems continuously analyze call traffic patterns, including call volume, frequency, duration, and cost anomalies, to identify suspicious activity.
- **Fraud Detection:** Machine learning algorithms flag behaviors indicative of robocalling, such as high-volume short-duration calls or calls to numbers on Do Not Call (DNC) lists.
- **Spam Call Reports:** Our softswitch generates daily reports to identify and block invalid or spoofed Automatic Number Identifications (ANIs).
- **Dynamic Blocking:** We maintain an updated database of known robocallers and implement real-time blocking of suspicious numbers or traffic patterns.

Call Blocking and Filtering

To mitigate robocall traffic:

- **Do Not Originate (DNO) Blocking:** We block calls from numbers on DNO lists, including those associated with government impersonation or one-ring scams.
- **Reputation Scoring:** We use call reputation scoring to identify and block calls from numbers associated with fraudulent activity or listed in the FCC consumer complaint database.
- **Invalid ANI Blocking:** Our softswitch automatically blocks calls with invalid or unallocated ANIs.
- **High-Risk Traffic Controls:** We apply dynamic blocking mechanisms to high-risk traffic routes based on behavioral analysis.

Traceback Cooperation

We are fully committed to cooperating with the FCC, law enforcement, the Industry Traceback Group (ITG), and other authorized entities to investigate and stop illegal robocallers. Our commitments include:

- **24-Hour Response:** We respond to all traceback requests within 24 hours, providing detailed call records, subscriber information, and technical assistance.

- **Dedicated Contact:** Our Network Operations Center (NOC) is the primary point of contact for traceback inquiries:
 - **Contact Title:** Fraud Mitigation Team
 - **Contact Phone:** +1 914-216-9292
 - **Contact Email:** noc@mysmartws.com
 - **Company Name:** Smart Telecard Inc
 - **Name:** Hanif Bhagat
 - **Title:** CEO
 - **Address:** 1091 Yonkers Avenue, Yonkers, NY 10704
- **Enforcement Actions:** If a customer is identified as originating illegal robocalls, we take immediate action, including warning the customer, implementing mandatory account codes, restricting call destinations, or terminating service.

Customer Education and Reporting

We actively educate our customers about robocall regulations and the consequences of non-compliance through:

- **Service Agreements:** Clear guidelines in our TOS outline permissible uses of our services.
- **Training Materials:** We provide resources to help customers understand their responsibilities in preventing illegal robocalls.
- **User-Friendly Reporting:** Customers can report suspicious or unwanted calls through our dedicated portal. Our fraud team investigates these reports promptly and takes appropriate action.

Upstream Provider Vetting

We maintain relationships only with upstream providers registered in the Robocall Mitigation Database. We have:

- Reviewed their Robocall Mitigation Plans to ensure compliance with FCC regulations.
- Established contractual agreements that require adherence to STIR/SHAKEN and robocall mitigation standards.
- Limited the number of upstream providers to ensure traceability and accountability.

Network Capacity Management

To prevent network abuse:

- **Capacity Limits:** We establish concurrent call capacity limits for each customer based on their service needs, such as the number of endpoints and average call usage.
- **Trunk Restrictions:** Individual trunks are capped to prevent excessive call origination.

- **Monitoring and Expansion:** We monitor call traffic to ensure capacity limits are appropriate and expand them only for verified, legitimate use cases.

Third-Party Validation

We partner with third-party validation services to enhance our ability to identify and block illegal robocalls. These services provide advanced analytics to detect suspicious call patterns and verify caller identities. If potentially illegal traffic is identified, we block the respective subscriber until further investigation confirms compliance.

Continuous Improvement

We are committed to continuously improving our robocall mitigation program by:

- Staying informed about emerging robocall threats and industry best practices.
- Participating in industry collaborations, including the ITG and other stakeholder groups.
- Regularly updating our systems, policies, and training programs to address evolving threats.
- Conducting periodic audits of customer traffic and compliance protocols.

Compliance with FCC Regulations

We certify that:

- All calls originating on our network are subject to this RMP.
- We have not been subject to formal FCC, law enforcement, or regulatory actions related to illegal robocalls or spoofing in the past two years.
- We will update our RMP submission in the Robocall Mitigation Database within 10 business days of any material changes.

Conclusion

Smart Telecard Inc's comprehensive Robocall Mitigation Plan reflects our unwavering commitment to preventing illegal robocalls and protecting consumers. By implementing STIR/SHAKEN, robust KYC procedures, advanced monitoring, and proactive cooperation with regulatory and industry entities, we strive to maintain a secure and trustworthy communication environment. We welcome feedback from the FCC and other stakeholders to enhance our efforts further.