

SMS-iT Robocall Mitigation Program Description

Submitted in compliance with 47 CFR § 64.6305 Requirements

I. Introduction and Certification Status

SMS-iT hereby submits this comprehensive robocall mitigation program description in compliance with 47 CFR § 64.6305(a). As a provider utilizing multiple telecommunications partners including Twilio, Plivo, SignalWire, Bandwidth, Telnyx, Ytel, Slooce, and Vonage, we certify that:

1. No prior certification has been removed by Commission action
2. We have not been prohibited from filing in the Robocall Mitigation Database
3. All calls originated on our network are subject to this robocall mitigation program
4. We have not implemented STIR/SHAKEN on any portion of our network

II. Call Analytics and Prevention Systems

A. Third-Party Analytics Integration

We utilize multiple analytics systems for comprehensive call monitoring:

- Twilio's fraud detection and prevention system
- Bandwidth's spam scoring
- Vonage's traffic analysis tools
- Partner carrier analytics platforms
- Real-time traffic pattern analysis systems

B. Traffic Monitoring and Analysis

Our monitoring system includes:

1. Real-time pattern recognition for suspicious traffic
2. Volume threshold monitoring and anomaly detection
3. Automated blocking of known bad actors
4. Spam content filtering
5. Integration with partner carrier monitoring systems

6. Continuous traffic quality assessment

III. Know Your Customer (KYC) and Customer Protection Procedures

A. Initial Customer Verification

1. Legal business documentation verification
2. Tax ID and business registration validation
3. Authorized signatory verification
4. Physical address verification
5. Website and online presence review
6. Use case documentation
7. Volume projections assessment

B. Ongoing Customer Monitoring

1. Regular account reviews (minimum quarterly)
2. Traffic pattern analysis
3. Customer complaint monitoring
4. Compliance verification checks
5. Volume threshold monitoring
6. Regular customer information updates

IV. Preventive Measures

A. Pre-transmission Controls

1. Content filtering for known spam patterns
2. Volume limitations based on customer profile
3. Sender ID verification
4. Message format validation
5. Customer authentication requirements
6. Traffic pattern analysis

B. Active Controls

1. Real-time traffic monitoring
2. Automated suspension of suspicious activities
3. Multi-layer authentication
4. Regular security audits
5. Immediate mitigation capabilities
6. Customer notification system

V. Partner Integration and Upstream Provider Due Diligence

A. Active Partnership Management

We maintain active partnerships with:

- Twilio
- Plivo
- SignalWire
- Bandwidth
- Telnyx
- Ytel
- Slooce
- Vonage

B. Partnership Compliance Requirements

For each partner, we maintain:

1. Current compliance documentation
2. Verification of RMD registration
3. Service quality metrics
4. Regular compliance reviews
5. Shared threat intelligence
6. Coordinated response protocols

VI. 24-Hour Traceback Response Protocol

A. Dedicated Response Team

- 24/7 availability
- Multiple contact methods
- Dedicated compliance staff
- Backup personnel assignments

B. Response Procedures

1. Immediate acknowledgment (within 1 hour)
2. Full response within 24 hours
3. Detailed call record access
4. Caller information retrieval
5. Traffic pattern analysis
6. Mitigation action documentation

VII. Documentation and Record Keeping

We maintain comprehensive records including:

1. All customer verification documents
2. Traffic monitoring logs
3. Mitigation actions taken
4. Traceback request responses
5. Investigation results
6. Training records
7. Policy updates
8. Compliance reports

VIII. Training and Updates

Our program includes:

1. Regular staff training on compliance requirements

2. Updates to mitigation procedures based on new threats
3. Documentation of all training sessions
4. Industry best practices review
5. Regular team certifications
6. Compliance update distributions

IX. Commitment Statement

SMS-iT explicitly commits to:

1. Respond fully to all traceback requests within 24 hours
2. Cooperate with the Commission, law enforcement, and industry traceback consortium
3. Take immediate action on identified illegal traffic
4. Maintain accurate and current documentation
5. Update this program as regulations evolve
6. Provide regular compliance reports
7. Maintain open communication with regulatory bodies

X. Contact Information

Primary Contact

Compliance Department

Email: [mgt@smsit.ai]

Phone: 650-488-9899 and 415-524-6028 [24/7 Compliance Hotline]

Address: 1392 Market Street, STE 200, San Francisco, CA 94102, United States

Secondary Contact

Legal Department

Email: [legal@smsit.ai]

Phone: 415-524-6028

This program description is submitted in compliance with 47 CFR § 64.6305 requirements and will be updated as needed to maintain compliance with FCC regulations.