

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Filer Information:

- **Filing Entity:** NajmX LTD
- **FRN:** 0037632502
- **Date:** 11/21/2025

1. OVERVIEW

This document describes the comprehensive robocall mitigation program implemented by “**NajmX LTD**” to prevent the origination of illegal robocall traffic on our network. Our program is designed to comply with 47 CFR § 64.6305(a) and includes reasonable steps to avoid originating illegal robocall traffic, along with a commitment to respond fully and within 24 hours to all traceback requests.

2. KNOW YOUR CUSTOMER (KYC) AND ONBOARDING PROCEDURES

2.1 Customer Verification Process

- Business Registration Verification: All customers must provide valid business registration documents, including business license, tax identification number, and proof of business address.
- Identity Verification: For individual customers, we require government-issued photo identification and verification of residential address.
- Contact Information: We collect and verify primary contact information, including business email, phone number, and mailing address.

2.2 Service Agreement Requirements

- All customers must execute a service agreement that explicitly prohibits:
 - * Illegal robocalling
 - * Call spoofing
 - * Telemarketing violations (TCPA, TSR compliance)
 - * Fraudulent or deceptive calling practices
- Agreements include acknowledgment of potential service termination for violations.

2.3 Customer Due Diligence

- We conduct background checks on new customers, including verification of business legitimacy.
- We review customer websites, business profiles, and public records.
- We maintain records of all customer verification documents for audit purposes.

3. CALL MONITORING AND ANALYTICS

3.1 Real-Time Call Monitoring

- Call Pattern Analysis: Our systems monitor calling patterns in real-time to identify:
 - * Unusually high call volumes
 - * Short call durations (potential robocall indicators)
 - * Rapid sequential dialing patterns
 - * Geographic anomalies
 - * Call completion rates

3.2 Automated Detection Systems

- We utilize automated analytics to flag suspicious calling behavior, including:
 - * Calls per minute/hour thresholds
 - * Answer rate monitoring and Call duration analysis
 - * Destination number pattern analysis

3.3 Network Monitoring

- Continuous monitoring of network traffic through our dialer systems
- Integration with upstream provider analytics where available.
- Daily review of call statistics and anomaly reports.

4. INVESTIGATION PROCEDURES

4.1 Alert Response

- When suspicious calling patterns are detected, our support team is immediately notified.
- Initial investigation begins within 2 hours of detection.
- All flagged accounts are reviewed by our compliance team.

4.2 Investigation Process

- Step 1: Review customer account details and service history
- Step 2: Analyze calling patterns and call records
- Step 3: Contact customer for explanation and documentation
- Step 4: Review customer's compliance with service agreement
- Step 5: Determine if activity is legitimate or requires action

4.3 Documentation

- All investigations are documented with date and time of detection, details of suspicious activity, customer response (if any), actions taken, and resolution status.

5. ENFORCEMENT ACTIONS

5.1 Warning Procedures

- First-time violations may result in a written warning and requirement to provide compliance documentation.
- Customers are given 24-48 hours to respond and demonstrate compliance.

5.2 Service Restrictions

- For confirmed violations or failure to respond, we may implement call volume restrictions, require additional verification, or place account under enhanced monitoring.

5.3 Service Termination

- Immediate Termination: Services will be immediately blocked and terminated if:
 - * Customer is using services for illegal robocalling
 - * Customer is engaged in call spoofing or fraud
 - * Customer fails to respond to traceback requests
 - * Customer violates TCPA or other telemarketing regulations
 - * Customer provides false or misleading information

5.4 Blocking Procedures

- Upon determination of illegal activity, we immediately suspend all services to the customer, block all associated DIDs and phone numbers, notify upstream providers of the termination, and maintain records of termination for future reference.

6. TRACEBACK COMMITMENT

6.1 24-Hour Response Commitment

We commit to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission (FCC), law enforcement agencies, the Industry Traceback Consortium (ITC), and other authorized entities.

6.2 Traceback Procedures

- Receipt: All traceback requests are logged immediately upon receipt
- Investigation: We investigate the call in question using our call records and customer information
- Response: We provide complete information including customer identification, call details and records, account status, and any relevant documentation
- Cooperation: We fully cooperate with investigating entities to stop illegal robocallers

6.3 Traceback Contact Information

- **Primary Contact:** Alaa Hesham
- **Email:** alaa.hesham@najmx.net
- **Phone:** +201113695203
- **Availability:** 24/7 for urgent traceback requests

7. THIRD-PARTY VENDORS AND UPSTREAM PROVIDERS

7.1 Upstream Provider Relationships

We work with multiple upstream voice service providers, including Tier 1 carriers and established VoIP service providers. All upstream providers are carefully vetted to ensure they maintain their own comprehensive robocall mitigation programs and comply with FCC requirements, including STIR/SHAKEN implementation where applicable.

7.2 Vendor Compliance

- We require all upstream providers to maintain their own robocall mitigation programs and demonstrate compliance with FCC regulations
- We monitor upstream provider compliance and performance on an ongoing basis
- We maintain the right to switch providers if they fail to meet compliance standards or demonstrate inadequate robocall mitigation practices
- We conduct regular reviews of our upstream provider relationships to ensure continued compliance

7.3 Internal Systems

- Dialer Platforms: We operate and maintain dialer systems
- DID Management: We assign and manage DIDs for our customers
- Call Center Management: We provide call center infrastructure and management services

8. CONTINUOUS IMPROVEMENT

8.1 Program Updates

- We regularly review and update our mitigation program to address new threats and regulatory requirements
- We stay informed of FCC guidance and industry best practices
- We participate in industry forums and compliance training

8.2 Staff Training

- All staff members are trained on robocall mitigation procedures
- Regular updates are provided on new regulations and enforcement actions
- Compliance team receives specialized training on investigation procedures

9. RECORD KEEPING

9.1 Documentation Requirements

- We maintain records of all customer onboarding and verification documents, call monitoring reports and alerts, investigation records and outcomes, enforcement actions taken, and traceback request responses.

9.2 Retention Policy

- All records are retained for a minimum of 2 years
- Records are stored securely and are accessible for audit purposes
- Records may be retained longer if required by law or ongoing investigations

10. CERTIFICATION

We certify that:

- All calls originated on our network are subject to this robocall mitigation program
- We have implemented reasonable steps to avoid originating illegal robocall traffic
- We commit to respond fully and within 24 hours to all traceback requests
- We will cooperate fully with the Commission, law enforcement, and the industry traceback consortium
- We will investigate and take action to stop any illegal robocallers using our service

Prepared by: Alaa Hesham

Title: CEO

Date: 11/21/2025

Company: NajmX LTD