

Joonto, Inc. Robocall Mitigation Plan

I. Introduction

Joonto, Inc. is a Mobile Virtual Network Operator (MVNO) providing SMS, voice, and mobility services to enterprise clients, wholesale partners, and consumers. Joonto is committed to full compliance with the Federal Communications Commission (FCC) regulations to prevent and mitigate illegal robocalls, ensure customer protection, and maintain the integrity of U.S. telecommunications networks.

II. FCC Certification and Requirements

- Joonto certifies compliance with the FCC's Robocall Mitigation Database requirements.
- All outbound traffic is routed only through authorized carriers that support STIR/SHAKEN call authentication protocols.
- Joonto files and maintains updated certifications with the FCC and updates its Commission Registration System profile within 10 business days of any material change.
- Ryan Lambert, Chief Legal Officer, is the designated Chief Compliance Officer (CCO), with oversight authority for this plan.

III. Know Your Customer (KYC) Obligations

A. Individual Customers:

For Individual Customers, we require the customer's Legal name and 2 of the following 4 pieces of information:

- Legal name
- Date of birth
- Billing address
- Government-issued photo ID (driver's license, passport, state ID)
- SSN (last 4 digits, for U.S. customers)

Verification Steps:

- At least 2 of 4 elements verified via third-party vendors (e.g., Stripe).
- Photo ID authenticity validation.
- Address verification (USPS/CASS, AVS).
- SSN4 check with identity verification vendor.
- Mobile OTP confirmation before activation.

B. Business Customers

- Required Information:
- Legal entity name and EIN/Tax ID
- D&B Number
- Business address

- Authorized representative's government-issued ID
- Contact phone/email
- Verification Steps:
 - Entity validation via Secretary of State or registry.
- EIN/Tax ID verification.
- Verification of authorized representative identity.

C. Additional Fraud and Security Protections

- Screening against OFAC/sanctions lists.
- SIM-swap and port-out fraud prevention (locks on suspicious activity).
- Address and payment method verification (AVS, CVV, ACH micro-deposits).
- Record retention for minimum of 5 years.
- Enhanced due diligence for: High-volume callers, Resellers and aggregators, International customers, Customers with complaint history.

IV. Monitoring Mechanisms

- Real-Time Monitoring: Continuous analysis of call metadata to identify anomalies.
- Traffic Analysis: High-volume, short-duration call detection, invalid caller ID checks, geographic distribution analysis.
- Machine Learning & AI: Pattern recognition, scam signature detection, reputation scoring.
- Traceback Cooperation: Full participation in the USTelecom Industry Traceback Group with 24-hour response commitment.
- Blocking Protocols: Calls identified as definitively illegal (spoofing, scam, or flagged via traceback) will be blocked with documented evidence and customer notification procedures.

V. Compliance Procedures

- Certification: Joonto certifies its compliance annually with the FCC.
- Recordkeeping:
 - Customer verification evidence (5 years)
 - Call detail records (18 months minimum)
 - Monitoring activities and enforcement actions
- Enforcement Actions:
 - Suspension or termination of customers originating illegal robocalls.
 - Escalation to compliance/legal team.
 - Customer appeal process in cases of blocking.
- Liability Acknowledgment: Joonto accepts full responsibility for enforcing effective mitigation measures.

VI. Training and Oversight

- Annual training for all customer-facing staff on KYC, fraud detection, and robocall compliance.
- Specialized training for technical staff on STIR/SHAKEN and traffic monitoring.
- Compliance oversight by Ryan Lambert, Chief Legal Officer (CCO), reporting quarterly to the CEO and semi-annually to the Board of Directors.

VII. Consumer Protection and Transparency

- Clear disclosures in compliance with truth-in-billing requirements.
- Customer notifications for blocked calls (via portal, email, or SMS).
- Opt-out and consent management in compliance with TCPA requirements.
- Privacy protection of Customer Proprietary Network Information (CPNI) in line with FCC rules.

VIII. Continuous Improvement and Review

- Quarterly robocall mitigation effectiveness reviews.
- Annual compliance audits with internal and external oversight.
- Program updates within 30–60 days of significant regulatory or operational changes.

IX. Compliance Framework.

9.1 Joonto, Inc. hereby certifies its full implementation of and compliance with the STIR/SHAKEN call authentication framework as mandated by the Federal Communications Commission (FCC) pursuant to the TRACED Act and related FCC Orders.

9.2. Authentication Implementation.

9.2. 1. Joonto has implemented the STIR/SHAKEN protocols across its entire network infrastructure to authenticate and verify the accuracy of caller ID information for all calls originated on its network.

9.2.2. All calls originated through Joonto's network receive appropriate attestation levels (A, B, or C) based on the company's relationship with and knowledge of the call originator.

9.2.3. Joonto maintains secure, private key infrastructure to digitally sign all SIP INVITE messages for calls originated on its network in accordance with industry standards.

9.3. Verification Procedures.

9.3.1. Joonto verifies STIR/SHAKEN authentication information on all calls received from other voice service providers where such information is available.

9.3.2. Calls lacking proper authentication or failing verification are subject to enhanced scrutiny through the monitoring mechanisms detailed in Section IV of this Plan.

9.4. Attestation Level Assignment.

9.4.1. a Level Attestation: Assigned to calls where Joonto has established a direct relationship with the customer, can verify the customer's right to use the calling number, and has implemented robust Know Your Customer procedures as outlined in Section III.

9.4.2. b Level Attestation: Assigned to calls where Joonto has established a relationship with the customer but cannot verify with certainty the customer's right to use a specific calling number.

9.4.3. c Level Attestation: Assigned to calls received from interconnected providers where the call source cannot be fully determined.

9.5. Technical Implementation.

9.5. 1. Joonto has deployed the necessary infrastructure to support the PASSporT token format and SIP Identity header mechanisms as specified in ATIS-1000074, ATIS-1000080, and ATIS-1000084.

9.5.2. Joonto maintains secure connections with the Secure Telephone Identity Policy Administrator (STI-PA) and approved Secure Telephone Identity Certification Authorities (STI-CAs) for certificate management.

9.6. Compliance Certification and Reporting.

9.6.1. Joonto has registered with the FCC's Robocall Mitigation Database and certified its STIR/SHAKEN implementation status.

9.6. 2. Joonto will update its certification in the Robocall Mitigation Database within 10 business days of any material change to its STIR/SHAKEN implementation.

9.6. 3. Joonto maintains comprehensive records of its STIR/SHAKEN implementation, including technical specifications, testing results, and operational procedures, for a minimum of 24 months.

9.7. Ongoing Compliance and Improvement.

9.7. 1. Joonto conducts quarterly reviews of its STIR/SHAKEN implementation to ensure continued compliance with evolving industry standards and FCC requirements.

9.7.2. Technical staff receive specialized training on STIR/SHAKEN protocols and implementation at least annually.

9.7.3. The Chief Compliance Officer oversees STIR/SHAKEN compliance as part of the overall robocall mitigation strategy.

X. Certification

Joonto, Inc. certifies that this Robocall Mitigation Plan:

- Meets FCC requirements, including the Robocall Mitigation Database.
- Integrates robust KYC and monitoring mechanisms.
- Ensures accountability and oversight through its Chief Compliance Officer.
- Will be continuously reviewed and updated to reflect industry best practices and evolving FCC requirements.

Approved by:

Tyler Kizerian, President

Ryan Lambert, Chief Legal Officer & Chief Compliance Officer

Date: August 23, 2025