

SECURE UICC CORP. ROBOCALL MITIGATION PLAN RMD

File No.: RMD0004752

Date: April 2, 2026

I. Company Overview and Role in the Call Chain

Secure UICC Corp. ("Secure UICC") is a Mobile Virtual Network Operator (MVNO) that functions as a **voice service provider**. We provide voice, text, and data services directly to our customers, including call origination, routing, and termination on our network. We originate calls placed by our end-user customers and process calls on the Internet Protocol (IP) portions of our network. We do not act as a gateway provider or non-gateway intermediate provider.

II. Robocall Mitigation Program – Specific Reasonable Steps

Secure UICC maintains a comprehensive robocall mitigation program designed to prevent, detect, and stop illegal robocall traffic at every stage. The program is based on the three required elements for voice service providers and is actively enforced.

1. Affirmative, Effective Measures to Prevent New and Renewing Customers from Originating Illegal Robocalls

- **Customer Vetting & Onboarding Process:** Every new customer and every renewing customer must complete a multi-factor verification process that includes: (a) government-issued photo ID, (b) proof of physical business or residential address, (c) business registration documents (if commercial), and (d) a detailed description of intended calling patterns and use cases. High-risk customers (e.g., telemarketing, high-volume outbound) receive additional manual review and references.
- **Contractual Prohibitions:** All customer service agreements explicitly prohibit the origination of illegal robocalls, spoofing, or any traffic that violates the Telephone Consumer Protection Act (TCPA) or FCC rules. Violations result in immediate service suspension and termination.
- **Ongoing Monitoring & Blocking:** Customer traffic is monitored in real time. Accounts showing indicators of illegal activity (e.g., >50% short-duration calls, high answer-seizure ratios to DNC-listed numbers, repetitive dialing patterns, or sudden spikes in call volume) are automatically flagged for review and blocked within minutes. Blocked customers receive notice and an appeal process, but service is not restored until the issue is resolved to our satisfaction.

- **Renewal Reviews:** Prior to any service renewal, we re-verify customer legitimacy and review recent traffic analytics.

2. Call Analytic Systems Utilized

- **Internal Analytics Platform:** We operate a proprietary real-time call analytics system that analyzes every originated call for:
 - STIR/SHAKEN attestation levels (A/B/C) and verification results.
 - Call duration, answer/seizure ratio, and unique called-number ratios.
 - Geographic calling patterns and velocity (calls per minute).
 - Correlation with known robocall “signatures” from industry threat intelligence feeds.
- **Third-Party Tools:** We integrate industry-standard third-party analytics services that provide robocall scoring, reputation databases, and anomaly detection (specific vendor names and contracts are available to the FCC upon request for confidentiality reasons).
- **Response Protocol:** Any call or customer flagged as high-risk by the analytics system is automatically routed to a manual review queue. Confirmed illegal traffic is blocked at the network edge, and the originating customer is notified and suspended.

3. Procedures to Know Our Upstream Providers

- **Due-Diligence Process:** We maintain formal, ongoing relationships only with upstream providers (host Mobile Network Operators and any intermediate carriers) that:
 - Maintain a valid, current certification in the FCC Robocall Mitigation Database, and
 - Have demonstrated effective robocall mitigation practices.
- **Contractual Requirements:** All upstream agreements require the provider to (a) implement STIR/SHAKEN, (b) maintain their own robocall mitigation program, (c) respond to traceback requests within 24 hours, and (d) immediately notify us of any suspected illegal traffic.

- **Periodic Reviews:** We review the RMD status and public enforcement actions against each upstream provider at least quarterly. We maintain direct 24/7 contact information for traceback and mitigation coordination.
- **Traffic Management:** We monitor inbound and outbound traffic with upstream partners and will cease routing with any provider that fails to meet our mitigation standards.

III. Additional Required Elements of the Mitigation Program

- **STIR/SHAKEN Implementation:** We have fully implemented STIR/SHAKEN on all IP portions of our network and assign appropriate attestation levels (A/B/C) based on customer verification.
- **Traceback Commitment:** Secure UICC certifies that it will respond **fully and completely** to every traceback request within **24 hours** of receipt, including providing all requested call detail records and customer information permitted by law.
- **Record-Keeping:** We retain all mitigation-related records (analytics logs, blocking actions, customer vetting documents, and traceback responses) for a minimum of two years.
- **Program Review:** This robocall mitigation plan is reviewed and updated annually (or more frequently if FCC rules or threat landscapes change) by senior management.

Secure UICC is committed to full compliance with all FCC robocall mitigation rules and to protecting the integrity of the U.S. telephone network.

Signed:

Casey Hardiman

Support Lead

Secure UICC Corp. Date: April 2, 2026