

TriceTel, Inc.

Robocall Mitigation Program Description

Doing Business As (DBA):	CoverageX Mobile
Filing Type:	Federal Communications Commission (FCC) Robocall Mitigation Database (RMD)
Date of Implementation:	May 18, 2026
Document Version:	1.1 (Updated Executive Certification)

1. Purpose and Regulatory Commitment

TriceTel, Inc. d/b/a CoverageX Mobile ("CoverageX Mobile" or the "Company") is committed to preventing the origination and transmission of illegal, fraudulent, and malicious robocalls across its telecommunications network. This Robocall Mitigation Program Description ("Program") outlines the comprehensive technical, operational, and administrative controls implemented by the Company.

This Program is designed to fully comply with the Federal Communications Commission's (FCC) rules governing voice service providers, including the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Title 47 of the Code of Federal Regulations (C.F.R.) § 64.1200, and subsequent FCC Third Report and Order guidelines regarding Robocall Mitigation Database certifications.

2. STIR/SHAKEN Implementation & Network Architecture

CoverageX Mobile certifies that it has fully implemented the STIR/SHAKEN (Secure Telephone Identity Revisited / Signature-based Handling of Asserted information using toKENs) cryptographic authentication framework within its IP-based network architecture.

- **Attestation Standards:** The Company applies STIR/SHAKEN tokens to all SIP-based calls originating on its network. Calls receive an 'A' (Full), 'B' (Partial), or 'C' (Gateway) attestation based strictly on the strict verification of the customer's identity and their legal authorization to utilize the telephone number displayed in the Caller ID field.
- **Cryptographic Tokens:** The Company utilizes valid, authorized certificates obtained through an approved Certificate Authority recognized by the Secure Telephone Identity Governance Authority (STI-GA).
- **Non-IP Networks:** To the extent that any segment of the network utilizes legacy Time-Division Multiplexing (TDM) architecture where STIR/SHAKEN cannot be natively transmitted, the Company actively engages in robust robocall mitigation practices specifically tailored to TDM environments, ensuring comprehensive network safety.

3. Robust Customer Due Diligence (Know Your Customer / KYC)

A foundational pillar of CoverageX Mobile's robocall mitigation strategy is preventing bad actors from gaining access to its network infrastructure. The Company enforces stringent "Know Your Customer" (KYC) onboarding and monitoring protocols, which include:

- **Identity Verification:** Comprehensive verification of commercial legitimacy, including validation of corporate registration, Tax Identification Numbers (EIN), physical business addresses, and authorized corporate officers.
- **Service Usage Evaluation:** Thorough screening of a prospective customer's intended business use cases, expected call volume patterns, and source of telephone numbers prior to service provisioning.
- **Restriction on High-Risk Services:** Enhanced scrutiny and restrictive controls placed on wholesale traffic aggregators, automated dialer platforms, and entities utilizing highly dynamic or short-duration calling signatures.

4. Real-Time Analytics and Network Traffic Monitoring

CoverageX Mobile employs sophisticated, automated network monitoring systems designed to detect, isolate, and remediate anomalous traffic patterns indicative of illegal robocalling, spoofing, or telemarketing abuse.

A. Behavioral Pattern Detection

The network analytics platform constantly scans call detail records (CDRs) for established signatures of malicious robocalling, which include:

- Extremely high volumes of short-duration calls (calls lasting less than 6 seconds).
- High ratios of uncompleted calls, calls rejected by recipients, or calls to non-allocated/invalid telephone numbers.
- Massive bursts of concurrent calls originating from a single customer endpoint or IP address.
- Discrepancies in Caller ID fields, such as unassigned, unallocated, or invalid North American Numbering Plan (NANP) numbers.

B. Dynamic Thresholds and Mitigation Triggers

When any customer's traffic exceeds established behavioral thresholds, the platform triggers an immediate tiered response, including automated rate-limiting, temporary traffic suspension, and mandatory administrative review by the Network Operations Center (NOC).

5. Mandatory Response to Tracebacks and Federal Enforcement

Traceback Mandate Compliance: CoverageX Mobile fully cooperates with the Industry Traceback Group (ITG), the FCC, the Federal Trade Commission (FTC), and state Attorneys General. The Company guarantees a rapid, substantive response to all formal traceback requests, identifying the immediate upstream source or originating customer of the flagged traffic within twenty-four (24) business hours of receipt.

If an upstream wholesale provider or direct customer fails to cooperate with a traceback investigation or is found to be intentionally transmitting illegal traffic, CoverageX Mobile reserves the contractual and operational right to immediately terminate the interconnectivity or customer agreement without prior liability.

6. Enforcement, Enforcement Mechanisms, and Penalties

The Company strictly enforces a zero-tolerance policy for illegal robocalling activities. Violations of this Program or the Company's Acceptable Use Policy (AUP) result in swift corrective actions, which are systematically applied as follows:

- **Immediate Suspension:** Sudden, unexplained spikes in unauthorized or high-volume short-duration calls trigger an immediate automated or manual block of the offending trunks.
- **Contractual Termination:** Customers or downstream providers who generate verified illegal robocalls, fail KYC updates, or fail to respond to traceback inquiries are subject to immediate, permanent service termination.
- **Regulatory Reporting:** Where systemic or criminal fraud is uncovered, the Company will proactively report the findings and associated entity details to the FCC Enforcement Bureau and relevant law enforcement bodies.

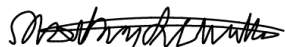
7. Periodic Review and Continual Program Enhancement

The telecommunications threat landscape is highly dynamic. To ensure that this Program remains consistently effective against evolving robocall techniques, the Compliance and Engineering departments of TriceTel, Inc. conduct a formal, comprehensive review of this Program at least annually.

This review assesses the technical efficacy of analytics thresholds, updates KYC criteria against emerging fraud trends, verifies certificate validity with the STI-GA, and adjusts network controls to maintain absolute alignment with ongoing statutory updates from the FCC.

8. Corporate Officer Certification

I hereby certify that I have reviewed the foregoing Robocall Mitigation Program Description and that TriceTel, Inc. d/b/a CoverageX Mobile maintains and adheres to the practices, procedures, and technical standards described herein to mitigate the origination and transmission of illegal robocalls.



Authorized Signature

Nathan Stratton

Founder, CTO

TriceTel, Inc. / CoverageX Mobile

05/18/2026

Date