

Robocall Mitigation Program (RMP)

Company Name: Trusted Technologies, LLC

Date of Implementation: 1/1/2026

Version: [e.g., 1.0]

1. Introduction and Program Purpose

Trusted Technologies, LLC (the "Company") is committed to preventing the origination of illegal robocalls and protecting the integrity of the public switched telephone network (PSTN). This Robocall Mitigation Program (RMP) outlines the specific, proactive steps the Company takes to ensure that its network is not used to transmit illegal or fraudulent voice traffic, in compliance with 47 C.F.R. § 64.6305.

2. STIR/SHAKEN Implementation Status

The Company has implemented the STIR/SHAKEN caller ID authentication framework as follows:

- **Implementation Level:** Full
- **Technical Methodology:** Our SIP trunk provider performs call attestation and applies SHAKEN Identity headers using certificate-based authentication. Calls are validated and attestation results are passed through the SIP signaling. No on-premise signing infrastructure is deployed..
- **Attestation Policy:** The Company assigns "A-Level" attestation only when the customer identity is verified and the customer has the legal right to use the telephone number in the Caller ID field.

3. Know Your Customer (KYC) Procedures

The Company prevents illegal robocalling at the source by performing rigorous due diligence on all new and existing customers.

- **Identity Verification:** Before service activation, we collect and verify Business Tax ID, and physical address.
- **Service Usage Review:** We require customers to describe their intended use case; e.g., Appointment Reminders, Retail Sales, ticket updates.
- **Contractual Prohibitions:** All service agreements include an "Acceptable Use Policy" (AUP) that strictly prohibits the transmission of illegal robocalls and provides for immediate termination for violations.

4. Traffic Monitoring and Analytics

The Company employs a multi-layered approach to monitor network traffic for patterns indicative of illegal robocalling.

- **Automated Monitoring:** Our systems flag traffic based on the following metrics:
 - **High Volume/Short Duration:** Excessive calls under 6 seconds in length.
 - **Low Completion Rates:** Call Answer-to-Seizure Ratios (ASR) falling below 20%.
 - **High Call Velocity:** More than 10 calls per minute from a single source.
- **Analytics Partnership:** We utilize Internal Tools to cross-reference traffic against known "do-not-originate" lists and suspicious caller ID databases.

5. Investigation and Traceback Cooperation

The Company acts swiftly when potential illegal activity is detected or reported.

- **Traceback Participation:** The Company fully cooperates with the Industry Traceback Group (ITG) and law enforcement. We commit to responding to all traceback requests within **[Insert Timeframe, e.g., 24 hours]**.
- **Enforcement Action:** If an investigation confirms illegal activity, the Company may:
 1. Issue a formal warning and require immediate remediation.
 2. Rate-limit or block specific traffic streams.
 3. Suspend or terminate the customer's service without notice.

6. Program Oversight and Contact Information

This program is reviewed at least annually to ensure effectiveness against evolving robocalling tactics.

Authorized Officer: Adam Pacchiana, President

Traceback Contact: 475-674-0175

Principal Place of Business: 355 Federal Road, Brookfield, CT 06804