



Robocall Mitigation Plan

Purpose

This **Robocall Mitigation Plan (RMP)** describes the policies, technical controls, operational procedures, and enforcement measures implemented by **Tini-Tech Solutions LLC** to detect, prevent, and mitigate illegal robocalls in compliance with **47 CFR § 64.6305**.

1. Provider Role and Operational Scope

- Company: Tini-Tech Solutions LLC
- Provider roles:
 - Originating Voice Service Provider (VSP)
 - Domestic Intermediate Provider
- Non-Gateway: Tini-Tech does not operate as a Gateway Provider.
- Domestic-only traffic: Tini-Tech does not accept or originate international ingress traffic; all traffic originates domestically from:
 - Direct retail customers, or
 - Vetted domestic wholesale partners.
- Network boundary: The company controls the IP-to-PSTN interconnection points from which calls are originated onto the PSTN.

2. STIR/SHAKEN Implementation and Attestation Governance

- Implementation: STIR/SHAKEN has been implemented on Tini-Tech's IP voice network per industry best practices.
- Attestation policy:
 - Attestation A (Full): Issued only when Tini-Tech has verified the customer's legal identity and authority to use the Calling Number (ANI) through documentation such as Letters of Authorization (LOA), direct numbering assignment records, or equivalent evidence.
 - Attestation B (Partial): Applied to vetted wholesale partners or resellers with an established business relationship (suitable KYC completed) where Tini-Tech cannot directly verify the customer's control of the specific ANI.
 - Attestation C (Gateway): Not used. As a domestic-only, non-gateway provider, Tini-Tech does not issue Attestation C.
- Certificate management: Private keys and certificates used for PASSPORT signing are stored and managed according to documented security controls; certificate renewal

and revocation procedures are defined in the company's internal CA operations document.

3. Robocall Mitigation Practices

Tini-Tech applies the following mitigation controls to all traffic, including portions where STIR/SHAKEN may not be fully deployed.

A. Customer Onboarding and Know-Your-Customer (KYC)

- Retail customers:
 - Identity verification using government-issued ID or equivalent, billing and contact information, and proof of authority to use any claimed telephone numbers.
 - Collection and retention of a signed Letter of Authorization (LOA) or other documentation when a customer claims control of third-party numbers.
- Wholesale partners and high-volume customers:
 - Enhanced Due Diligence (EDD) required prior to provisioning: business formation documents, tax ID/EIN, key contact information, and traffic use-case descriptions.
 - Traffic profile expectations documented (typical call volumes, geography, calling patterns). Acceptance contingent on pass of EDD.
- Denial criteria: Applicants with unverifiable identity, inconsistent use-case statements, or negative risk scores from third-party screening will be denied service.

B. Contractual and Acceptable Use Controls

- Service agreements include explicit terms prohibiting illegal robocalling, falsification of caller identity, and unauthorized use of third-party numbers.
- Contracts reserve the right to suspend or terminate service immediately for suspected illegal robocalling or violation of the RMP.
- Customers must permit lawful inspection and provide timely information for traceback investigations.

C. Real-Time Monitoring and Analytics

- Continuous monitoring of per-account and per-trunk metrics, including:
 - Calls per second (CPS)
 - Concurrent calls (CC)
 - Answer seizure ratio (ASR)
 - Average call duration (ACD)
 - Short-call rates and disconnect patterns
- Automated anomaly detection: Threshold-based and machine-learning models flag deviations from the customer's expected traffic profile.
- Third-party feeds: Integration with commercial risk scoring, blacklists, and reputation services to augment internal detection.
- Alerting: High-severity anomalies generate automated alerts to the Network Operations Center (NOC) for immediate action.

D. Call Filtering and Rate Controls

- Progressive mitigation steps:

- Rate limiting: Temporary throttles applied to trunks or accounts exhibiting suspicious surges.
- Challenge/response or CAPTCHA mechanisms where applicable (for SIP-originated traffic).
- Blocking: Routes or customers responsible for confirmed illegal traffic will be blocked from originating to the PSTN.
- “No-Signature, No-Route” enforcement for PSTN egress: Outbound calls lacking required STIR/SHAKEN signatures and proper attestation are blocked at the company edge, except where permitted by law or for calls from pre-authorized legacy TDM interconnects during transition periods.

E. Traceback and Incident Response

- Incident response process:
 - Triage: NOC investigates alerts within defined SLAs.
 - Containment: Apply immediate mitigations (rate-limits, route blocks, account suspension) if an incident is confirmed or strongly suspected.
 - Remediation: Require corrective actions from the customer or partner; escalate to termination for persistent or egregious violations.
- Law enforcement and industry cooperation:
 - Tini-Tech will respond to traceback requests from the FCC, Industry Traceback Group (ITG), and law enforcement in a timely manner—initial acknowledgement within 24 hours and substantive response/testing assistance per request timeline.
- Traceback records: Maintain detailed CDRs, SIP logs, and signaling information to support traceback efforts.

1. Enforcement, Escalation and Recordkeeping

- Enforcement steps:
 - Level 1: Automated rate limiting and alerts.
 - Level 2: Manual investigation and temporary suspension of suspect traffic.
 - Level 3: Permanent route blocking and service termination when illegal activity is confirmed.
- Customer notification: Affected customers will receive written notice describing the reason for mitigation and steps required for remediation; emergency mitigations may be applied without prior notice if required to protect the network.
- Record retention:
 - Maintain CDRs, onboarding documents (LOAs, KYC), incident tickets, and mitigation actions for a minimum of two years (or longer if required by law or regulatory guidance).
- Change control and audit:
 - Documented change-control process for updates to RMP, STIR/SHAKEN policies, and mitigation thresholds.
 - Periodic internal reviews and external audits as appropriate to verify RMP effectiveness.

2. Governance and Personnel

- Roles and responsibilities:
 - CEO / Authorized Representative: Overall responsibility for RMP compliance and signatory authority.

- Network Operations Center (NOC): Day-to-day monitoring and initial incident response.
- Security/Compliance Officer: KYC oversight, policy updates, and coordination with legal/law enforcement.
- Customer Success / Account Management: Onboarding, LOA collection, and customer communications.
- Training: Regular staff training on robocall regulations, traceback procedures, and RMP enforcement actions.

3. **Certification and Signatory**

I certify that the information contained in this Robocall Mitigation Plan is true and accurate, and that Tini-Tech Solutions LLC has implemented the controls described herein.

Company: Tini-Tech Solutions LLC
FCC Registration Number (FRN): 0037574647
Authorized Representative: Waleed Ghouri
Title: Owner / CEO
Business Address:
1500 N Grant St #5014
Denver, CO 80203
Date of Issuance: April 03, 2026