

Robocall Mitigation Program Description

For Submission to FCC Robocall Mitigation Database

Filing Entity: C.P. Technology Group, llc

FCC FRN: 0038072591

Date: February 1, 2026

Role in Call Chain: Voice Service Provider directly serving end-users (originating and terminating voice traffic to/from residential and business subscribers using NANP resources).

STIR/SHAKEN Implementation Certification:

- Fully implemented across all IP network segments (own SPC token and certificate from approved STI-PA/STI-CA; authenticating all eligible outbound calls with A/B/C attestation levels).

We certify that:

- All calls originated on our network are subject to this robocall mitigation program.
- We take reasonable steps to prevent/mitigate illegal robocalls (TCPA violations, Do Not Call, spoofing, etc.).
- We commit to fully respond to traceback requests from the FCC, law enforcement, or an industry consortium within 24 hours.
- No prior certification has been removed by Commission action, and we are not prohibited from filing in the RMD.

1. Customer Onboarding and Know-Your-Customer (KYC) Procedures (Required for VSPs per 47 CFR § 64.6305(d)(2)(ii) & § 64.1200(n)(4))

- All customers (residential/business) undergo verification during signup: government-issued ID, proof of address/utility bill, EIN/tax ID for businesses, and direct relationship confirmation.
- Customers must agree to terms prohibiting illegal robocalling/spoofing/telemarketing without consent; violation triggers immediate review/suspension.
- High-risk/high-volume customers (e.g., call centers, predictive dialers): Enhanced due diligence including call pattern previews, business references, proof of TCPA consent mechanisms, and contractual clauses for rapid termination.
- Ongoing monitoring for red flags (e.g., sudden volume spikes, complaints).

2. STIR/SHAKEN Caller ID Authentication Implementation

- Registered with STI-PA; hold valid SPC token and certificate (renewed proactively; monitor CRL/OCSP).
- Authenticate outbound IP-originated calls with U.S. NANP caller ID:
 - **A-level** (Full Attestation): For verified subscribers/enterprises with direct control/relationship.
 - **B-level** (Partial): Authenticated number but limited origination certainty.
 - **C-level** (Gateway/Unauthenticated): Minimized; used only where unavoidable (e.g., certain interconnected traffic).
- Attestation logic applied internally (no third-party certs used under our name).
- Verify inbound where feasible; display SHAKEN indicators to subscribers.
- Equivalent measures on any non-IP segments.

3. Traffic Monitoring, Analytics, and Call Blocking

- Deploy real-time/near-real-time analytics to detect patterns indicative of illegal robocalls:
 - Excessive short-duration calls, high answer/seizure ratios, and rapid sequential dialing.

- Calls to registered Do Not Call numbers, known spam targets, or invalid/unallocated numbers.
- Matching known scam campaigns (e.g., via industry data feeds).
- Maintain and apply **Do Not Originate (DNO)** lists (FCC-mandated, including public lists); block outbound use of listed numbers.
- Dynamic rules: Threshold-based blocking (e.g., >X calls/min per line → auto-review/suspend); reputation scoring of customers/numbers.
- Integrate traceback/consortium data for pattern recognition.

4. Response to Traceback Requests and Complaints

- Designated 24/7 point of contact: On Call Support, 1-804-601-0885, support@cptechgroup.com
- Commit to a full response within 24 hours to FCC, law enforcement, or industry traceback.
- Investigate consumer/other-provider complaints promptly; cooperate fully in stopping sources.

5. Call Blocking and Termination Policies

- Immediate suspension/termination upon credible evidence of illegal robocalling.
- Proactive blocking of suspected traffic to prevent downstream harm.
- Audit logs are maintained for all actions (available for FCC review).

6. Ongoing Compliance, Audits, and Updates

- Annual internal review of program effectiveness.
- Employee training on robocall rules/mitigation.
- Monitor FCC developments (e.g., RCD, verified caller name).
- Update RMD within 10 business days of changes (ownership, contacts, etc.).

This program is actively implemented and regularly reviewed. We do not knowingly originate/transmit illegal robocalls and take affirmative, effective measures to prevent such activity.