

Robocall Mitigation Strategy and Compliance Plan

Company: TELEPARS TELECOMMUNICATIONS CORP

Date of Implementation: 09/03/2025

Filing Date in RMD: 03/17/2022

1.0 Commitment and Overview

TELEPARS TELECOMMUNICATIONS CORP ("TELEPARS") is unequivocally committed to protecting consumers and our network from illegal robocalls and spoofing. This Robocall Mitigation Plan ("the Plan") details the comprehensive and reasonable steps we have implemented to prevent our network from originating illegal robocall traffic, as required by the Federal Communications Commission (FCC) under its rules and the TRACED Act.

TELEPARS certifies that this Plan is designed to significantly reduce the origination of illegal robocalls and that we adhere to the practices described herein. This Plan is filed in the FCC's Robocall Mitigation Database and will be enforced across all voice services we offer.

2.0 Know Your Customer (KYC) & Subscriber Verification

We implement robust Know Your Customer protocols to authenticate all subscribers before granting network access. Our KYC process is designed to verify the identity, legal status, and legitimacy of the business or entity seeking service to prevent bad actors from accessing our network.

- **New Subscriber Onboarding:** All new customers undergo a rigorous, multi-step identity validation process prior to service activation.
 - **Business Validation:** Prospective subscribers must provide valid business registration documents, tax identification numbers (EIN/SSN), and government-issued identification for authorized contacts.
 - **Address Verification:** A verification email and physical postcard are sent to confirm the validity of the provided business address and express consent to our terms. No service is activated until these verifications are returned.
 - **Telephone Registration:** Prospective subscribers providing information via phone receive an automated callback to the number provided to confirm its legitimacy and link it to the account.
 - **Risk Assessment:** New accounts are subject to a risk-based scoring system. Accounts flagged as high-risk (e.g., high-volume VoIP resellers) undergo

enhanced due diligence, including background checks and review of historical business practices.

- **Traceback Cooperation Commitment:** As a condition of service activation, all subscribers must contractually agree to cooperate fully with all lawful traceback investigations and commit to responding to traceback requests within twenty-four (24) hours when such information is requested from them by TELEPARS or authorized investigative bodies.
- **Existing Subscriber Authentication:** For ongoing use of our services, we employ a layered authentication system.
 - **Caller ID Authentication:** The system automatically recognizes calls originating from a subscriber's registered calling number.
 - **PIN-Based Authentication:** If a call originates from an unregistered number, the subscriber must provide a pre-established PIN to gain network access.
- **Audit Trail & Record Keeping:** All subscriber activity, including call originator specifications and KYC documentation, is comprehensively logged and retained for the duration of the business relationship and for a minimum of [Insert Retention Period, e.g., 24 months] thereafter to ensure full traceability.

3.0 Contractual Enforcement & Acceptable Use Policy

We bind all subscribers to strict contractual obligations that prohibit illegal calling activity.

- **Acceptable Use Policy (AUP):** All subscribers must agree to and sign our AUP prior to service activation. The AUP explicitly prohibits:
 - Originating illegal, fraudulent, or deceptive calls, including spoofing caller ID information.
 - Violating any applicable local, state, or federal telecommunications laws.
 - Engaging in activities that violate industry best practices and guidelines.
- **Enforcement Actions:** Our terms of service grant TELEPARS the right to take immediate action, including issuing warnings, suspending service, or terminating accounts for any violation of the AUP.

4.0 Caller ID Attestation & Number Authorization

We uphold the integrity of the STIR/SHAKEN caller ID authentication framework by strictly validating calling numbers.

- **Company-Provisioned Numbers:** For telephone numbers (TNs) directly managed and assigned by TELEPARS to a subscriber, validation is inherent. We maintain a secure inventory of all assigned numbers and monitor their use.
- **Customer-Bring-Your-Own-Numbers:** If a subscriber wishes to use a TN not managed by TELEPARS, they must provide a valid Letter of Authorization (LOA) from the number's assignee of record. We will only attest to calls using these TNs after successful validation of the LOA.
- **Attestation Decision:** Prior to originating any call, our system checks the calling party number against our authorized inventory. A call will not receive attestation if the number cannot be properly validated.

5.0 Network Monitoring & Dynamic Traffic Analytics

We proactively monitor network traffic using advanced analytics designed to detect patterns indicative of illegal robocalling.

Our systems analyze calling patterns in real-time, including:

- Anomalous call volumes and velocity (e.g., high-frequency, back-to-back calls).
- Deviations from established customer baselines and weekly trends.
- Abnormalities in call duration distributions.
- High volumes of calls to unique destination numbers in a short timeframe.
- Multiple simultaneous calls on a single account, suggesting potential account compromise.
- Unusual cost patterns generated by a single customer.

6.0 Investigation, Mitigation, & Traceback Cooperation

We maintain a dedicated risk prevention team to investigate and mitigate suspicious activity.

- **Investigation Procedures:** Upon alert from our monitoring systems or receipt of a complaint, our team initiates a formal investigation. This includes:
 - Analyzing call detail records (CDRs) against expected behavior.

- Reviewing account activity and history.
- Verifying call-origination paths.
- Contacting the subscriber to validate the activity.
- **Cooperation with Traceback Requests:** TELEPARS is fully committed to cooperating with all lawful traceback investigations. To ensure prompt action and compliance with industry standards:
 - **Response Commitment:** We commit to responding to all traceback requests (from law enforcement, the FCC, the Industry Traceback Group (ITG), and other investigative bodies) **within twenty-four (24) hours** of receipt. This response will include the requested call detail records, customer information, and origination details to the extent permissible by law.
 - **Subscriber Obligations:** We contractually require all subscribers to cooperate fully with traceback requests and to identify their upstream providers to facilitate end-to-end investigations.
 - **Single Point of Contact (SPOC):** We maintain a designated SPOC available 24/7 to ensure immediate and complete responses to emergency and standard traceback inquiries.
 - **Documentation:** All traceback requests and the actions taken in response are documented and retained for compliance auditing.
- **Mitigation Actions:** Confirmed illegal robocalling activity will result in immediate mitigation, including blocking specific calls, suspending service, or terminating the subscriber's account.

7.0 Call Blocking & Compliance

- TELEPARS will promptly implement and honor all Do Not Originate (DNO) requests received from the ITG and recognized industry entities.
- We employ mechanisms to automatically block calls identified as suspicious by our internal analytics and confirmed through investigation.

8.0 Plan Maintenance and Updates

The threat landscape of illegal robocalling is dynamic. Therefore, this Plan is a living document.

- TELEPARS will continuously monitor and incorporate evolving industry best practices.
- Any material changes to this Plan will be promptly communicated to all relevant employees, consultants, and contractors.
- An updated version of this Plan will be filed in the FCC's Robocall Mitigation Database within ten (10) business days of any material update.