

## FireTEXT Robocall Mitigation Plan

This Robocall Mitigation Plan (RMP) is submitted by **FireTEXT Dispatch Solutions**, pursuant to the provisions of **47 C.F.R. § 64.6305**, adopted by the Federal Communications Commission (FCC). This document outlines FireTEXT's current policies and procedures to prevent the origination and transmission of illegal robocalls on its network. FireTEXT is committed to responding to traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG) while cooperating with all entities in investigating and stopping illegal robocall activity.

---

### I. STIR/SHAKEN Implementation Status

FireTEXT has fully implemented the STIR/SHAKEN call authentication framework across its network, ensuring that all calls originating from our system are authenticated and verified to prevent illegal robocalls.

- **Full Implementation:**  
FireTEXT's network infrastructure supports SIP-based interconnected calls with full STIR/SHAKEN attestation, meeting the requirements set forth by the FCC under 47 CFR § 64.6305.
  - **Ongoing Compliance:**  
FireTEXT continually monitors and maintains its systems to ensure ongoing compliance with STIR/SHAKEN standards and proactively addresses any updates or changes to regulatory requirements.
- 

### II. Commitment to Respond to Traceback Requests

FireTEXT cooperates fully with the FCC, law enforcement, and the ITG in responding to traceback requests. Specifically:

- **Response Time:** All traceback requests will be addressed within 24 hours of receipt.
  - **Single Point of Contact:** FireTEXT has designated a single point of contact for handling traceback requests (see Appendix A).
  - **Contractual Obligations:** FireTEXT includes language in its service agreements requiring customers and upstream providers to cooperate fully with traceback requests.
- 

### III. Customer Vetting Practices

To prevent illegal robocalls from originating on our network, FireTEXT employs strict customer vetting procedures:

1. **Verification Process:**

- Collection of customer details, including physical address, federal tax ID, and business purpose.
- Verification of customer identity through signed agreements and supporting documentation.

## **2. Service Agreements:**

- FireTEXT includes acceptable use policies that explicitly prohibit using our services for illegal robocalls.
- Customers violating these terms may face suspension or termination of service.

## **3. Monitoring:**

- Continuous monitoring of customer traffic for patterns indicative of illegal robocall activity.

---

## **IV. Telephone Number Validation Practices**

FireTEXT ensures that every number used by our customers is validated:

- Only numbers directly managed or obtained through authorized partners are permitted.
- Systems are configured to screen and block numbers that do not match the customer's assigned numbers.

---

## **V. Ongoing Robocall Mitigation Practices**

FireTEXT uses proactive measures to detect and prevent illegal robocalls, including:

- 1. Traffic Monitoring:** Regular review of call detail records (CDRs) to identify patterns of suspicious activity, such as:
  - High call volumes in short timeframes.
  - Sequential dialing patterns.
  - Calls to invalid numbers or numbers on the Do Not Call Registry.
- 2. Traceback and Investigation:**
  - Immediate traceback investigation for flagged activity.
  - Verification of Caller ID ownership and origin.
- 3. Automated Tools:**
  - AI-driven call analytics to detect unusual call patterns.
  - Blocking mechanisms for known fraudulent or high-risk numbers.

---

## VI. Upstream Provider Cooperation

FireTEXT maintains robust relationships with upstream providers and requires all interconnection agreements to include:

- Commitments to mitigate illegal robocall activity.
- Cooperation in traceback investigations.

---

## VII. Third-Party Analytics

FireTEXT leverages third-party analytics platforms to strengthen its robocall mitigation efforts:

- **Call Analytics:**
  - Real-time monitoring and filtering of calls based on reputation scores and historical activity.
  - Use of blacklisting and whitelisting to prevent calls from known fraudulent sources.
- **Blocking Mechanisms:**
  - CAPTCHA-based gateways to distinguish human callers from autodialers.
  - Shield databases for screening calls against "Do Not Originate" lists.

---

## Appendix A: Contact and Provider Information

### Single Point of Contact for Traceback Requests:

- **Name:** John Cook
- **Title:** Vice President
- **Phone Number:** (870) 483-2535
- **Email Address:** [support@firetext.net](mailto:support@firetext.net)

### Upstream Provider Information:

- **Primary Provider:** Twilio
  - **Nature of Business:** SMS and Voice Services

---

FireTEXT remains committed to upholding the highest standards of compliance and integrity in robocall mitigation. For additional details or questions regarding this plan, please contact us at [support@firetext.net](mailto:support@firetext.net).