

# Robocall Mitigation & Call Authentication Program

---

## 1. Program Overview & Regulatory Foundation

**507 Communications LLC** maintains this Robocall Mitigation Program (the "Program") as a comprehensive, multi-layered framework designed to detect, prevent, and mitigate illegal robocall traffic traversing our network. This Program is a cornerstone of our commitment to network integrity and consumer protection, and is formally registered with the Federal Communications Commission (FCC) Robocall Mitigation Database (RMD).

The Program is guided by and operates in full compliance with the following regulatory and industry standards:

- **FCC Regulations:** Full implementation of the STIR/SHAKEN authentication framework (47 CFR § 64.6300 et seq.), the requirements of the TRACED Act, and active participation in the Industry Traceback Group (ITG) processes.
- **RMD Certification Requirements:** Adherence to all FCC RMD filing obligations, including mandatory annual recertification and the requirement to update our filing within **10 business days** of any material change to the information provided.
- **Mandatory Actions:** A firm commitment to respond fully to all traceback requests from the FCC, law enforcement, and the industry traceback consortium within **24 hours**.
- **Industry Best Practices:** We align our operational protocols with standards set by the ATIS/SIP Forum and the USTelecom Robocall Principles.

---

## 2. Core Mitigation & Authentication Measures

### 2.1 Real-Time Call Analytics & Monitoring

We deploy advanced analytics to identify and quarantine high-risk traffic in real time.

- **AI-Driven Anomaly Detection:** Our systems are programmed to detect patterns indicative of fraud, such as:
  - **Volume Spikes:** Sudden surges exceeding calls per hour from a single source.
  - **Geographic Anomalies:** Traffic originating internationally while spoofing domestic U.S. caller IDs.
- **Comprehensive Data Cross-Referencing:** Incoming and outgoing call data is cross-referenced against a range of dynamic threat intelligence sources:
  - **Do-Not-Originate (DNO) Lists:** We comply with FCC rules requiring the blocking of calls from numbers on reasonable DNO lists (e.g., government numbers that do not make outbound calls).
  - **FCC Consumer Complaint Database:** We monitor and act on numbers frequently reported in consumer complaints.

- **RMD Flagged Providers:** We screen for traffic from providers whose RMD certifications have been found deficient by the FCC.

## 2.2 Call Blocking & Mitigation Actions

We utilize a risk-based, graduated enforcement model to stop illegal calls before they reach consumers.

- **Tier 1 (High Risk - Immediate Blocking):** Calls are automatically blocked if they:
  - Originate from numbers listed on a DNO list.
  - Fail STIR/SHAKEN validation with a status of "Invalid" or "No Verification."
- **Tier 2 (Suspicious - Flagged for Manual Review):** Calls are flagged for further investigation if they exhibit:
  - Abnormally short call duration (e.g., less than 5 seconds, potentially "one-ring" scams).
  - Severe Caller ID/CNAM mismatches (e.g., a number displaying "IRS" that does not belong to a government agency).
- **Upstream/Downstream Collaboration:**
  - We actively participate in the traceback process, providing requested call data promptly.
  - We are committed to the **Know Your Upstream Provider (KYUP)** framework, meaning we vet our upstream partners and will cut off traffic from providers that enable illegal activity.

---

## 3. Network Security, Compliance, & Fraud Prevention

### 3.1 Know Your Customer (KYC) Protocols

To prevent bad actors from gaining access to our network, we enforce robust customer vetting procedures.

- **Customer Vetting:** All new customers (including business entities and VoIP resellers) are subject to rigorous KYC diligence, including validation of business licenses and EINs.
- **Enhanced Monitoring:** High-risk clients, such as call centers, are subject to enhanced scrutiny, including more frequent reviews of their traffic patterns.

### 3.2 Recordkeeping, Audits, and Recertification

We maintain detailed records to support our compliance posture and enforcement actions.

- **Log Retention:** Call Detail Records (CDRs) and records of all blocking actions are retained for a minimum of **2 years**.
- **Compliance Audits:** We undergo comprehensive third-party compliance audits on a **[Biannual/Annual]** basis.

### 3.3 Outreach and Regulatory Filings

We actively engage with consumers and regulators to support the broader fight against illegal robocalls.

- **Consumer Education:** We maintain a public-facing portal for robocall complaints and provide guides to consumers on enrolling in the FCC's "Do Not Call" registry.
  - **Regulatory Compliance:** We ensure all filings are current, including our annual RMD recertification. We remain current on all new FCC proposals and requirements, including those pertaining to caller ID display and foreign-originated calls.
- 

## 4. Point of Contact & Officer Certification

### 4.1 Robocall Mitigation Point of Contact

The individual designated to handle all robocall mitigation-related issues, including traceback requests, is:

- **Name:** Emily Watkins
- **Email:** support@507-communications.com
- **Phone:** (320) 317-6157