

Robocall Mitigation Plan

CLEAR TELECOM SOLUTIONS L.L.C Certification of Compliance with the TRACED Act & FCC Robocall Mitigation Rules

CLEAR TELECOM SOLUTIONS L.L.C certifies that it has implemented and maintains a **Robocall Mitigation Program** in full compliance with **47 CFR § 64.6305** to prevent illegal robocalls, spoofing, and fraudulent traffic originating from or transiting its network. This plan outlines policies, procedures, and technical measures to ensure adherence to FCC regulations.

Certification Statements

1. Implementation of Robocall Mitigation Measures

- CLEAR TELECOM SOLUTIONS L.L.C maintains a comprehensive program to detect, prevent, and eliminate illegal robocalls and spoofing.
- Measures include **call authentication (STIR/SHAKEN where applicable), call blocking, subscriber vetting, and network monitoring.**

2. Regulatory Compliance

- Neither CLEAR TELECOM SOLUTIONS L.L.C nor its affiliates have:
 - Been subject to **FCC enforcement actions, civil penalties, or sanctions** related to illegal robocalling.
 - Received **findings of misconduct, false certifications, or deficiencies** from the FCC, law enforcement, or traceback groups.

Robocall Mitigation Practices

1. Traceback Cooperation

- **Designated Point of Contact**
 - A **24/7 traceback contact** (name, title, address, phone, email) is registered in the **FCC Robocall Mitigation Database** for prompt responses.
- **Response to Traceback Requests**
 - Acknowledge and investigate requests **within 24 hours.**

- Provide **call records, logs, and subscriber information** to assist in identifying illegal robocallers.
- Take **corrective action** (suspension/termination) against bad actors.

2. Subscriber Vetting & Identity Verification

- **Customer Due Diligence**

- Verify all subscribers (residential, business, wholesale) with:
 - **Government-issued ID**, business registration (if applicable), and address confirmation.
 - Review of prior fraud/robocall violations.

- **Enhanced Screening for High-Risk Customers**

- Outbound call centers, VoIP resellers, and high-volume users undergo:
 - **Additional documentation** (proof of legitimate business).
 - **Ongoing call monitoring** for suspicious spikes in traffic.
 - **Contractual prohibitions** against illegal robocalling.

3. Caller ID Authentication & Validation

- **Authorized Number Usage**

- Subscribers may **only use CLEAR TELECOM SOLUTIONS L.L.C-assigned numbers** (no unauthorized spoofing).
- **Single-line users** must call from their assigned number.
- **Multi-line (MLTS) users** must ensure calls originate from pre-authorized numbers.

- **Caller ID Authentication & Blocking**

- Uses **STIR/SHAKEN (where implemented) and third-party analytics**.
- In **Iowa**, employs **Aureon's CIDA with Outbound Shield** to:
 - Block **spam, invalid, or unallocated numbers**.
 - Apply **dynamic call blocking** based on threat intelligence.

4. Network Monitoring & Illegal Traffic Prevention

- **Real-Time Traffic Analysis**

- Automated systems detect:
 - **Sudden call volume spikes.**
 - **Short-duration calls** (indicative of robocalling).
 - **Calls to known fraud-associated numbers.**

- **Mitigation Actions**

- **Immediate investigation** by security teams.
- **Warning, suspension, or termination** of suspicious accounts.

5. Know-Your-Customer (KYC) Policy for Carriers

- **Carrier Vetting**

- Upstream providers must:
 - Be **registered in the FCC Robocall Mitigation Database.**
 - Provide **business identification** (legal name, address, compliance history).

- **Contractual Compliance**

- All agreements include:
 - **Prohibitions on illegal robocalling/spoofing.**
 - **Mandatory cooperation with traceback requests.**
 - **Right to terminate service for violations.**