

Robocall Mitigation Plan

C&T TELECOMMUNICATION POWER SOLUTIONS

Certification of Compliance with the TRACED Act & FCC Robocall Mitigation Rules

C&T TELECOMMUNICATION POWER SOLUTIONS 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 the policies, procedures, and technical measures in place to mitigate unlawful robocalls and ensure adherence to FCC regulations.

Certification Statements

1. Implementation of Robocall Mitigation Measures

- **C&T TELECOMMUNICATION POWER SOLUTIONS** has established a **comprehensive Robocall Mitigation Program** designed to detect, prevent, and eliminate illegal robocalls and caller ID spoofing across its network. This includes **call authentication (STIR/SHAKEN where applicable), call blocking, subscriber vetting, and network monitoring** to ensure compliance with FCC rules.

2. Regulatory Compliance

- **C&T TELECOMMUNICATION POWER SOLUTIONS** affirms that neither it nor any affiliated entities under its ownership, management, or control have:
 - Been subject to **FCC enforcement actions, civil penalties, or regulatory sanctions** related to illegal robocalling, spoofing, or robocall mitigation violations.
 - Received findings of **misconduct, false certifications, or deficiencies** in robocall mitigation efforts by the FCC, law enforcement, or industry traceback groups.

Robocall Mitigation Practices

1. Traceback Cooperation

- **Designated Point of Contact**
 - As mandated under **47 CFR § 64.6305(d)(4)(v)**, **C&T TELECOMMUNICATION POWER SOLUTIONS** maintains a **24/7 traceback contact** (name, title,

business address, direct phone number, and dedicated email) registered in the **FCC Robocall Mitigation Database**. This ensures prompt response to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG).

- **Response to Traceback Requests**

- **C&T TELECOMMUNICATION POWER SOLUTIONS** commits to:
 - **Acknowledging and investigating** traceback requests **within 24 hours** of receipt.
 - **Providing all necessary call records, logs, and subscriber information** to assist in identifying illegal robocallers.
 - **Taking immediate corrective action**, including service suspension or termination, against bad actors using its network.

2. Subscriber Vetting & Identity Verification

- **Customer Due Diligence**

- **All subscribers (residential, business, and wholesale)** undergo **identity verification** before service activation, including:
 - **Valid government-issued ID, business registration documents (if applicable), and service address confirmation.**
 - **Review of customer history** for prior fraudulent activity or robocall violations.

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

- **Outbound call centers, VoIP resellers, and high-volume users** are subject to:
 - **Additional documentation requirements**, such as proof of legitimate business operations.
 - **Ongoing call pattern monitoring** to detect sudden spikes in call volume or suspicious traffic.
 - **Contractual obligations** prohibiting illegal robocalling, with penalties for violations.

3. Caller ID Authentication & Validation

- **Authorized Number Usage**
 - **Subscribers may only use numbers assigned by C&T TELECOMMUNICATION POWER SOLUTIONS or its authorized partners.** Unauthorized spoofing or number manipulation is strictly prohibited.
 - **Single-line subscribers** are restricted to calling from their **assigned number (TDM or IP-based)**.
 - **Multi-line (MLTS) subscribers** must ensure all calls originate from **pre-authorized numbers**, with systems in place to detect and block unauthorized Caller ID use.
- **Caller ID Authentication & Call Blocking**
 - **C&T TELECOMMUNICATION POWER SOLUTIONS employs third-party analytics and STIR/SHAKEN (where implemented)** to verify caller ID legitimacy.
 - In **Iowa service areas, Aureon's Caller Identification Authentication (CIDA) with Outbound Shield** is used to:
 - **Block calls** from numbers flagged as spam, invalid, or unallocated.
 - **Apply dynamic call blocking** based on real-time threat intelligence.

4. Network Monitoring & Illegal Traffic Prevention

- **Real-Time Traffic Analysis**
 - **Automated systems continuously monitor call traffic** for anomalies, including:
 - **Sudden increases in call volume.**
 - **Short-duration calls indicative of robocalling.**
 - **Calls to numbers associated with fraud complaints.**
- **Mitigation Actions**
 - **Suspicious activity triggers:**
 - **Immediate investigation** by the network security team.
 - **Warning or suspension** of suspicious accounts pending review.

- **Permanent termination** of repeat offenders or confirmed bad actors.

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

- **Carrier Vetting**

- **All upstream providers and intermediate carriers must:**

- **Be registered in the FCC Robocall Mitigation Database.**
- **Provide valid business identification**, including:
 - Legal business name, physical address, and primary contact information.
 - State of incorporation and regulatory compliance history.

- **Contractual Compliance**

- **All interconnection agreements include:**

- **Explicit prohibitions** on illegal robocalling, spoofing, and fraudulent traffic.
- **Mandatory cooperation with traceback requests** and FCC investigations.
- **Right to terminate service** for violations of robocall mitigation policies.