

Robocall Mitigation Plan

BURRUS COMMUNICATIONS, INC.

Certification of Compliance with the TRACED Act and FCC Regulations

BURRUS COMMUNICATIONS, INC. hereby certifies that it has implemented and maintains a **Robocall Mitigation Program** in full compliance with **47 CFR § 64.6305**, governing all originating calls on its network.

Certification Statements

1. Implementation of Robocall Mitigation Measures

- **BURRUS COMMUNICATIONS, INC.** has established and enforces a **Robocall Mitigation Program** to prevent illegal robocalls and spoofing across its network.

2. Regulatory and Legal Compliance

- Neither **BURRUS COMMUNICATIONS, INC.** nor any affiliated entities under its ownership, management, or control have been subject to:
 - **FCC, law enforcement, or regulatory actions** related to illegal robocalling or caller ID spoofing.
 - **Findings of misconduct** regarding robocall mitigation certifications or program deficiencies.

Robocall Mitigation Practices

1. Traceback Cooperation

a. Designated Point of Contact

- As required under **47 CFR § 64.6305(d)(4)(v)**, **BURRUS COMMUNICATIONS, INC.** maintains a **24/7 traceback contact** (name, title, address, phone, and email) registered in the **FCC Robocall Mitigation Database**.

b. Response to Traceback Requests

- **BURRUS COMMUNICATIONS, INC.** commits to:
 - Responding to **FCC, law enforcement, and traceback consortium requests** within **24 hours**.

- Fully cooperating to **identify, investigate, and terminate** illegal robocallers using its network.

2. Subscriber Vetting & Identity Verification

a. Customer Due Diligence

- **Residential, retail, and wholesale subscribers** are verified using **standard business practices**, including:
 - Collection of **service address and identity documentation**.

b. Enhanced Screening for High-Risk Customers

- **Outbound call centers & high-volume users** undergo:
 - **Stricter application reviews** to prevent misuse.
 - **Ongoing monitoring** for suspicious calling patterns.

3. Caller ID Authentication & Validation

a. Authorized Number Usage

- Subscribers may **only use numbers assigned by BURRUS COMMUNICATIONS, INC. or authorized partners**.
- **Single-line subscribers**:
 - Calls are restricted to their **assigned number** (TDM or IP).
- **Multi-line (MLTS) subscribers**:
 - **All originating calls** are screened to ensure numbers match authorized assignments.

b. Caller ID Authentication

- **BURRUS COMMUNICATIONS, INC.** employs **third-party analytics** to detect and block illegal robocalls.
- In **Iowa service areas**, **Aureon's Caller Identification Authentication (CIDA) with Outbound Shield** is used to:
 - Block calls from **spam-listed or invalid numbers**.

4. Network Monitoring & Illegal Traffic Prevention

a. Real-Time Traffic Analysis

- **Anomalous calling patterns** are flagged for investigation.
- **High-volume traffic** is scrutinized for robocall indicators.

b. Mitigation Actions

- **Suspicious activity** triggers:
 - **Immediate investigation.**
 - **Termination of offending subscribers or carriers.**

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

a. Carrier Vetting

- **All upstream providers** must be **registered in the FCC Robocall Mitigation Database.**
- **Basic identification details** are collected, including:
 - Business address, contact person(s), state of incorporation, and business nature.

b. Contractual Compliance

- **All interconnection agreements** include:
 - **Prohibited traffic clauses.**
 - **Traceback cooperation requirements.**