

Robocall Mitigation Plan

DIGITAL TELECOM SYSTEMS, LLC

This document serves as the official **Robocall Mitigation Program** for DIGITAL TELECOM SYSTEMS, LLC, establishing our comprehensive framework for preventing illegal robocalls, caller ID spoofing, and fraudulent communications across our network. This plan demonstrates our full compliance with the **TRACED Act** and all applicable **FCC regulations (47 CFR § 64.6305)**, outlining the specific policies, procedures, and technical safeguards we have implemented to protect consumers and uphold telecommunications industry standards.

Certification Statement

DIGITAL TELECOM SYSTEMS, LLC hereby formally certifies the following commitments and compliance status:

1. Robocall Mitigation Commitment

- DIGITAL TELECOM SYSTEMS, LLC has developed, implemented, and continuously maintains a **robust Robocall Mitigation Program** designed to systematically prevent, detect, and eliminate illegal robocall traffic originating from or transiting through our network infrastructure. This program incorporates multiple layers of protection including advanced call authentication protocols, comprehensive subscriber verification processes, real-time network monitoring systems, and cooperative traceback procedures.

2. Regulatory Compliance Status

- DIGITAL TELECOM SYSTEMS, LLC affirms that neither our organization nor any affiliated entities under common ownership, management, or operational control have:
 - Been subject to any **formal FCC enforcement actions, investigations, or civil penalties** related to illegal robocalling, caller ID spoofing, or violations of robocall mitigation requirements.
 - Received any findings of **actual or suspected misconduct, fraudulent certifications, or program deficiencies** from the Federal Communications Commission, law enforcement agencies, or authorized industry traceback groups regarding our robocall mitigation efforts.

- Been identified as originating or facilitating unlawful robocall campaigns through regulatory audits or industry traceback investigations.

Comprehensive Robocall Mitigation Practices

1. Traceback Cooperation Framework

DIGITAL TELECOM SYSTEMS, LLC maintains a fully operational traceback response system that exceeds FCC requirements for cooperation with regulatory and law enforcement investigations:

- **Designated Traceback Contact**
 - We have established and registered in the **FCC Robocall Mitigation Database** a dedicated 24/7/365 traceback contact point consisting of:
 - Primary and secondary contact persons with clearly defined roles
 - Complete business contact information including physical address
 - Multiple direct communication channels (phone, email, secure portal access)
 - Escalation procedures for urgent requests
- **Comprehensive Response Protocol**
 - Our traceback response team is trained and equipped to:
 - Immediately acknowledge receipt of all traceback requests (within 1 hour of notification)
 - Initiate full investigations within 24 hours of request receipt
 - Provide complete call detail records, subscriber information, and network routing data
 - Preserve all relevant evidence for regulatory or legal proceedings
 - Implement immediate corrective actions including service suspension for confirmed violations

2. Multi-Layered Subscriber Vetting System

DIGITAL TELECOM SYSTEMS, LLC employs a tiered subscriber verification process designed to prevent bad actors from accessing our network:

- **Standard Identity Verification**

- All residential, business, and wholesale subscribers undergo rigorous pre-service verification including:
 - Government-issued photo ID validation through certified verification services
 - Business registration documentation for commercial accounts
 - Physical service address confirmation via multiple verification methods
 - Comprehensive review against known fraud databases and industry watchlists

- **Enhanced Due Diligence for High-Risk Segments**

- Certain subscriber categories face additional scrutiny:
 - **Outbound call centers:** Must provide proof of TCPA compliance, call scripts, and calling schedules
 - **VoIP resellers:** Required to submit complete business ownership documentation
 - **High-volume users:** Subject to traffic pattern analysis and periodic audits
 - All high-risk subscribers sign enforceable agreements with strict prohibitions against illegal calling practices

3. Advanced Caller ID Authentication System

DIGITAL TELECOM SYSTEMS, LLC has implemented a sophisticated caller ID validation framework:

- **Number Authorization Controls**

- Strict policies govern telephone number usage:
 - Subscribers may only use numbers directly assigned by DIGITAL TELECOM SYSTEMS, LLC

- Number porting requests undergo enhanced verification
- All number assignments are recorded in our centralized numbering database
- **Technical Enforcement Mechanisms**
 - Our network infrastructure enforces these policies through:
 - **Single-line subscribers:** Class 5 switch configuration restricts calling to assigned number only
 - **MLTS environments:** Session Border Controllers validate originating numbers against authorized lists
 - Real-time SIP header analysis to detect number spoofing attempts
- **Call Blocking Technologies**
 - DIGITAL TELECOM SYSTEMS, LLC utilizes multiple call validation solutions:
 - STIR/SHAKEN implementation where technically feasible
 - Third-party analytics platforms with real-time threat intelligence
 - In Iowa markets: Aureon's CIDA with Outbound Shield providing:
 - Dynamic blocking of invalid, unallocated, and flagged numbers
 - Reputation-based call filtering using constantly updated databases

4. Proactive Network Monitoring Program

DIGITAL TELECOM SYSTEMS, LLC operates a 24/7 Network Operations Center with specialized robocall monitoring:

- **Real-Time Traffic Analysis**
 - Automated systems continuously monitor for:
 - Abnormal call volume patterns (spikes, bursts, etc.)
 - Short-duration call anomalies
 - Suspicious destination number clusters
 - Invalid SIP messaging patterns

- **Threat Response Protocol**

- Detected anomalies trigger our mitigation workflow:
 1. Immediate alert to security team
 2. Temporary traffic restrictions pending investigation
 3. Subscriber notification and verification process
 4. Permanent termination for confirmed violations
 5. Reporting to industry databases and regulators

5. Carrier Relationship Management

DIGITAL TELECOM SYSTEMS, LLC maintains strict oversight of all carrier partnerships:

- **Upstream Provider Vetting**

- All intermediate carriers must:
 - Be properly registered in FCC databases
 - Maintain valid operating authority
 - Pass our financial and operational due diligence
 - Demonstrate robocall mitigation capabilities

- **Contractual Safeguards**

- All interconnection agreements include:
 - Explicit prohibitions on illegal traffic
 - Mandatory cooperation clauses
 - Audit rights and termination provisions
 - Liability for violations