



Tennessee Wireless Robocall Mitigation Program Description

This is the Tennessee Wireless, LLC robocall mitigation program for a non-gateway intermediate provider that only offers voice service bundled with its internet service and operates exclusively on its own IP network.

1. Scope and Applicability

This program applies to all voice traffic carried or processed on our private IP network infrastructure. As a non-gateway intermediate provider, we do not originate or terminate calls for external customers. Our voice service is exclusively offered as a bundled feature to customers who subscribe to our internet service, and all call traffic is confined to our company-owned and operated IP address range.

2. Reasonable Steps to Mitigate Illegal Traffic

To avoid carrying or processing illegal robocall traffic, we implement the following measures:

Network Access Control: Only authenticated, paying internet customers are permitted to initiate or receive voice calls through our system. Unauthorized devices or external SIP traffic are blocked at the network perimeter.

Traffic Monitoring: We continuously monitor call patterns (e.g., call volume, duration, destination) for anomalies indicative of robocalling. Automated systems flag and quarantine suspicious traffic for review.

IP-Based Routing: All calls are routed exclusively through our internal IP network. We do not peer with or accept traffic from external voice providers, eliminating third-party call sources.

Customer Acceptable Use Policy (AUP): Our AUP prohibits the use of our services for illegal robocalling or spoofing. Violations result in service suspension or termination.



3. Traceback Response and Cooperation

We commit to:

Respond to all traceback requests from the FCC, law enforcement, and the industry traceback consortium within 24 hours.

Provide complete and accurate call detail records (CDRs) and subscriber information for any investigated call.

Fully cooperate with authorities in identifying and stopping illegal robocallers using our network.

4. Certification and Compliance

We will file and annually update our certification in the FCC's Robocall Mitigation Database, confirming that:

All calls on our network are subject to this mitigation program.

We meet the requirements of 47 CFR § 64.6305(c).

A designated company officer is responsible for robocall mitigation compliance.