

Robocall Mitigation Program Description (Planned STIR/SHAKEN Implementation)

Company Name: Aeronet Wireless Broadband

Filing Type: Voice Service Provider – Robocall Mitigation Program (STIR/SHAKEN Implementation in Progress)

Date: 11/21/2025

1. Overview

Aeronet Wireless Broadband is a voice service provider committed to complying with the FCC's robocall mitigation requirements as outlined in 47 CFR § 64.6305. We are currently in the process of implementing the STIR/SHAKEN call authentication framework and have begun the required steps for obtaining certificates, configuring our signing infrastructure, and completing integration with our STIR/SHAKEN service provider, **TransNexus**.

While the STIR/SHAKEN deployment is being completed, we have implemented an interim Robocall Mitigation Program designed to prevent the origination of illegal robocalls on our network.

2. Planned STIR/SHAKEN Implementation

We are actively implementing STIR/SHAKEN and expect full deployment for all eligible SIP traffic following the below plan:

2.1 Implementation Steps Underway

- Acquisition of an **SPC token** and completion of STI-PA/CA onboarding.
- Integration of **TransNexus STIR/SHAKEN services** for call signing and verification.
- Testing and validation of:
 - SIP Identity header insertion
 - Certificate validation
 - Attestation level assignment
- Deployment and verification on production systems.

2.2 Expected Completion

We expect STIR/SHAKEN to be fully operational within the required FCC timelines following approval of our Robocall Mitigation Database filing.

3. Interim Robocall Mitigation Measures (Until STIR/SHAKEN Is Live)

While full STIR/SHAKEN implementation is pending completion, Aeronet Wireless Broadband is actively performing the following mitigation measures:

3.1 Know-Your-Customer (KYC) Policies

We validate all customers originating voice traffic by:

- Verifying business identity and contact information
- Reviewing intended use cases
- Screening for high-risk call patterns
- Ensuring acceptance of our anti-robocall and lawful use policies

3.2 Outbound Call Traffic Monitoring

We continuously monitor customer traffic to detect:

- High-volume or short-duration call patterns
- Abnormal spikes inconsistent with prior behavior
- Potentially illegal robocall signatures
- Repetitive dialing to large blocks of numbers

Traffic flagged as suspicious triggers an internal review and potential enforcement action.

3.3 Enforcement Actions

When questionable or illegal traffic is detected, we take immediate action, including:

- Blocking specific call attempts
- Rate-limiting outbound traffic
- Requiring customer remediation
- Suspension or termination of service for non-compliant customers

4. Traceback Cooperation

Aeronet Wireless Broadband fully cooperates with the **Industry Traceback Group (ITG)** and promptly responds to all traceback requests.

We retain call detail records (CDRs), customer assignment data, and relevant logs to support traceback investigations.

5. Ongoing Compliance and Review

- This program will be updated as STIR/SHAKEN implementation progresses.
 - Once deployed, STIR/SHAKEN authentication will replace interim measures for all eligible IP traffic.
 - We perform periodic compliance reviews to ensure alignment with FCC regulations.
-

6. Contact Information

Robocall Mitigation/Compliance Contact:

Name: Luis Cintron Roman

Title: Director of Network Engineering

Email: lcintron@aeronetpr.com

Phone: 787-273-4143 ext 214