

TRUE WIRELESS, INC.

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

As of March 2026

Pursuant to 47 CFR § 64.6305, True Wireless, Inc. ("Company") submits this report regarding its STIR/SHAKEN implementation posture and its Robocall Mitigation Program.

I. Company Background

True Wireless, Inc. is a wireless reseller that relies on underlying carrier partners to provide network access and voice service to its subscribers. Company does not own, operate, or control network switching infrastructure.

Company provides wireless service primarily to individual consumers, including participants in the federal Lifeline program. Services are intended for single-line personal use and are not structured for high-volume outbound calling.

II. STIR/SHAKEN Implementation Status

True Wireless, Inc. does not independently implement STIR/SHAKEN call authentication.

Company does not:

- Operate its own STIR/SHAKEN authentication servers
- Maintain an STI certificate
- Assign attestation levels to calls
- Control authentication headers

Instead, Company relies on its underlying carrier partners operating on the T-Mobile and AT&T networks to authenticate and sign eligible outbound voice calls in accordance with FCC rules and industry standards.

Underlying Carriers Responsible for Authentication:

1. T-Mobile USA, Inc.

FRN: 6945950

RMD Filing ID: RMD0004209

2. AT&T Mobility Services LLC

FRN: 21840798

RMD Filing ID: RMD0003903

III. Robocall Mitigation Program

A. Subscriber Due Diligence

- Subscriber identity verification procedures
- Acceptable Use Policy prohibiting unlawful robocalling
- Suspension/termination for violations (including Lifeline compliance)

B. Network-Level Mitigation & Carrier Controls

- Reliance on upstream STIR/SHAKEN authentication
- Network-level traffic monitoring and anti-spam analytics
- Cooperation with upstream mitigation actions

In addition to reliance on upstream STIR/SHAKEN authentication, True Wireless relies on its underlying carrier partners' network-level traffic monitoring, call analytics, spoof detection, and automated blocking tools to identify and mitigate suspicious or potentially unlawful calling patterns. True Wireless cooperates with its carrier partners in investigating abnormal traffic patterns and will suspend or terminate service where appropriate in accordance with its Acceptable Use Policy and applicable FCC rules.

C. Responding to Traceback Requests

- Dedicated point of contact
- 24-hour response commitment
- Investigation and documentation of suspicious activity

D. Recordkeeping

- Retention of relevant records for a minimum of 24 months

IV. Cooperation with Law Enforcement and Regulators

Company certifies that it is not currently subject to a formal Commission, law enforcement, or regulatory agency action related to unlawful robocalling or spoofing and has not been subject to such action within the past two years.

V. Certification

True Wireless, Inc. certifies that it takes reasonable and systematic measures to prevent the origination of illegal robocalls, relies on upstream carrier infrastructure for STIR/SHAKEN authentication, and complies with 47 CFR § 64.6305.