

AMPTelecom – Robocall Mitigation Program Description

1. Identification / STIR/SHAKEN Implementation Status

- **Company Name:** AMPTelecom
 - **Type of Provider:** Voice Service Provider
 - **STIR/SHAKEN Status:**

AMPTelecom has fully implemented the STIR/SHAKEN authentication framework on the IP portions of its network under its control, in compliance with **47 C.F.R. § 64.6301(a)(1)–(2)**. All calls we originate on these portions are signed and attested appropriately.

For any portions of the network where STIR/SHAKEN cannot be deployed due to lack of control over necessary infrastructure, no extension is claimed under § 64.6304, and AMPTelecom applies the mitigation steps described below.
-

2. Reasonable Steps to Avoid Carrying or Originating Illegal Robocall Traffic

A. Customer Vetting (“Know Your Customer”)

- AMPTelecom requires all new customers to undergo identity and legitimacy verification, including:
 - Valid government-issued business registration or personal identification.
 - Expected call patterns, volumes, and use cases.
 - For wholesale and reseller accounts: proof of regulatory authorization, compliance history, and disclosure of any prior enforcement or traceback requests.
- Customer agreements expressly prohibit origination of unlawful robocalls and caller-ID spoofing. Violations are grounds for immediate suspension or termination.

B. Call Traffic Monitoring and Analytics

- AMPTelecom uses both in-house systems and third-party analytics to:
 - Monitor call volumes for anomalies (e.g., short-duration high-volume calling, sequential dialing, high failure rates).
 - Flag suspicious caller-ID patterns or calls inconsistent with customer profiles.
 - Maintain updated blocklists and industry intelligence feeds to prevent known bad actors from originating traffic.

C. Mitigation and Blocking Measures

- Upon detection of suspicious traffic, AMPTelecom will:
 - Notify the customer immediately and investigate the activity.
 - Require corrective action within a short timeframe.
 - Suspend or block call traffic if the customer fails to remediate.
- Logs are maintained for all enforcement actions and flagged call streams.

D. Traceback and Investigations

- AMPTelecom responds to **all traceback requests within 24 hours**, as required by § 64.6305(d)(2)(iii).
- Dedicated compliance staff are assigned to support traceback activities and maintain call metadata to facilitate investigations.

3. Cooperation Commitment

- AMPTelecom fully cooperates with the **FCC, the Industry Traceback Group, and law enforcement authorities** in all investigations of suspected unlawful robocalls or spoofing.

- Data relevant to traceback (including timestamps, calling/called numbers, and routing details) are preserved and produced promptly when requested.
-

4. Regulatory / Enforcement History

- In the past two years, neither AMPTelecom nor any commonly owned or affiliated entity has been the subject of any enforcement action, formal investigation, or adverse finding related to illegal robocalling, spoofing, or deficient mitigation/certification.
-

5. Contact Information

- **Robocall Mitigation Contact:**
Edward Barrett Tribe
Officer, AMPTelecom

Phone: 512-600-1163 ext 2000
Email: barrett@amptelecom.com
-

6. Officer Certification

I, **Edward Barrett Tribe**, a duly authorized officer of **AMPTelecom**, hereby certify under penalty of perjury that the above-described robocall mitigation program is true and complete to the best of my knowledge, that AMPTelecom has fully implemented STIR/SHAKEN on all IP portions of its network under its control, and that AMPTelecom has adopted reasonable steps to avoid carrying or originating illegal robocall traffic, including committing to respond to all traceback requests within 24 hours and to cooperate with investigations by the Commission, law enforcement, and the industry traceback consortium.