

WooSender Robocall Mitigation Plan

1. STIR/SHAKEN Implementation

WooSender does not control numbering resources and does not directly implement STIR/SHAKEN. All call authentication and attestation are performed by our underlying carrier, **Bandwidth Inc., Twilio, and Plivo**, which has fully implemented STIR/SHAKEN in accordance with FCC requirements. WooSender relies on Bandwidth's implementation for originating, signing, and validating calls.

2. Customer Vetting and Onboarding

WooSender provides an AI-driven lead management and communications platform that allows clients to engage with their opted-in contacts via calls and text messages. To mitigate the risk of unlawful robocalls:

- All clients must agree to WooSender's Terms of Service, which prohibit illegal robocalling and require compliance with the Telephone Consumer Protection Act (TCPA) and related FCC rules.
- New accounts are screened through identity verification, payment verification, and internal compliance checks prior to activation.
- Accounts are subject to suspension or termination for suspected spam, high complaint rates, or violations of FCC/FTC telemarketing rules.

3. Monitoring and Enforcement

WooSender actively monitors account usage patterns (volume, frequency, complaint triggers) to detect potential spam or unlawful activity. If suspicious traffic is identified:

- WooSender investigates the account activity.
- Reports are escalated to Bandwidth, Twilio, and Plivo, who maintains ultimate authority over network-level blocking and disconnection.
- WooSender cooperates fully with Bandwidth, traceback requests from the Industry Traceback Group (ITG), and any FCC enforcement inquiries.

4. Compliance Contact

Name: Salvatore Garbesi

Title: Chief Technical Officer

Email: sal@woosender.com

Phone: 610.590.9576