

Robocall Mitigation Program Description Submitted to the Federal Communications Commission (FCC)

Company Name: Robotalker.com

FCC Registration Number: 0031422272

Contact Information: Thomas Mahoney, CEO, Thomas@Robotalker.com. 954-903-0834

RoboTalker.com LLC is a 15+ years old, small, family-owned VoIP platform dedicated to helping small businesses, churches, and property-managers to communicate effectively with their customers. We provide an affordable, web-based automated calling interface allowing legitimate organizations, such as appointment reminders, emergency alerts, and service updates. Our clients include churches (e.g., event announcements), property managers, lawn services (e.g., scheduling confirmations), healthcare providers appointment reminders (HIPAA-compliant), utilities companies (e.g., outage notifications and billing reminders) for automated calling. We offer Text-to-Speech in multiple languages, ringless voicemails, and opt-in management and opt-out processes are built into our system allowing opt-out for caller via "press 9 to no longer receive these calls" prompting.

We have always adhered strictly to FCC regulations, including TCPA consent requirements, we request in our terms that clients provide DNC scrubbing for interstate, non-opt-in calling, and we require them to keep their customer contact information up to date and phone numbers current, ensuring 100% legal operations as stated on our site (robotalker.com/legal-automated-calls).

Much of our traffic is business to business, which is outside the scope of the DNC and all FCC regulations for automated phone calls.

Exemption from STIR/SHAKEN Compliance:

- The rule that exempts RoboTalker.com LLC from STIR/SHAKEN compliance is 47 CFR § 64.6304(a), which provides an extension of the implementation deadline for small voice service providers. This rule defines a "small gateway voice service provider" with 100,000 or less voice service subscriber lines (aggregated over all affiliates). RoboTalker.com LLC qualifies as a small provider under this definition, operating as a low-volume, non-facilities-based platform with a limited subscriber base focused on small business clients. Our operations emphasize customer notifications rather than high-volume traffic, and we rely on third-party carriers for origination and termination, making full STIR/SHAKEN implementation disproportionately burdensome due to costs (e.g., SPC token acquisition, network upgrades) relative to our scale.
- Although the initial extension expired on June 30, 2023, we have not implemented STIR/SHAKEN on any portion of our network, as permitted under Option 3 for providers who certify a robust robocall mitigation program in lieu of authentication. This exemption applies because:

- We meet the size threshold (<100,000 lines), serving niche small business needs without large-scale subscribers.
- Our low-volume, notification-focused traffic poses minimal risk of illegal calls, as evidenced by our adherence to FCC rules since inception.
- The calls that originate on our network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a), which include reasonable steps to avoid originating illegal robocall traffic and include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls. We certify that any prior certification has not been removed by Commission action and we have not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that we have not implemented the STIR/SHAKEN authentication framework on any portion of our network.
- We have not been subject to FCC removal from prior certifications or prohibited from filing in the RMD.
- This aligns with FCC policy to allow small providers to prioritize mitigation over full framework adoption, as detailed in the Sixth Report and Order (FCC 23-18) and Wireline Competition Bureau guidance (DA 24-73).

Robocall Mitigation Program Description (Per 47 CFR § 64.6305(a)):

- RoboTalker.com LLC has implemented a comprehensive robocall mitigation program designed to take reasonable steps to avoid originating illegal call traffic. This program includes multi-layered fraud prevention at signup, login, content creation, and call origination stages, tailored to our low-volume notification services. We commit to responding fully and within 24 hours to all traceback requests from the FCC, law enforcement (e.g., FBI, state AGs), and the Industry Traceback Group (ITG), providing all requested data (e.g., CDRs, IP logs, user details). We also commit to cooperating fully in investigations, including suspending or terminating accounts implicated in illegal activity and sharing mitigation insights with industry partners. Our program is reviewed quarterly and updated as needed to address emerging threats, ensuring seamless compliance for our small business clients.

Pre-Signup Verification (Preventing Fraudulent Accounts):

- Credit Card Validation: We perform random undercharging (e.g., \$0.01–\$0.99) on credit cards to verify ownership and detect stolen cards. Failed validations block activation of their robotalker.com account entirely.
- Identity and Contact Validation: Emails are validated via confirmation links required to be accepted in the welcome email; social media profiles are cross-checked for authenticity (e.g., age, activity level); and phone calls are made to confirm user identity and intent, focusing on small business legitimacy (e.g., verifying church, property management and healthcare use cases). Suspicious patterns (e.g., mismatched data) trigger denial.

- Geographic and Network Filters: IP addresses are filtered to block high-risk regions (e.g., known VPNs or fraud hotspots via GeoIP databases). Time zone mismatches (e.g., signup at odd hours from overseas) flag for manual review. In 2025, this prevented ~15% of suspicious signups, protecting our notification-focused ecosystem.
- Post-Signup and Login Monitoring (Ongoing User Authentication):
- VIP Tier System: New users start as non-VIP with strict limits (e.g., 500 calls/day, 5,000/week) to align with low-volume needs. VIP status is awarded after 30–60 days of clean history, personal interviews (via video call to assess legitimacy, e.g., confirming property manager operations), and reference checks. This ensures only vetted small businesses access higher limits.
- Session-Based Filters: Each login triggers IP and time zone checks; anomalous behavior (e.g., multiple logins from different countries) suspends access pending verification. We log all sessions for traceback, emphasizing secure notifications for clients like utilities.

Content and Call Scheduling Safeguards (Detecting Illegal Traffic):

- Automated Word Filtering: All Text-to-Speech (TTS) inputs and audio uploads are scanned for 100+ prohibited terms/phrases associated with scams (e.g., "IRS," "loan," "winner," "fraud," "credit card", "payday"). Uploaded AUDIO FILES are automatically converted via Speech-to-Text (STT) for analysis filtering with the same bad word list resulting in account suspension. Our custom C# function, BadWordCheck(string Speech To Text), flags matches and auto-suspends the user's account: BadWordCheck.cs
- In 2025, this has flagged and suspended ~5% of uploads, safeguarding notifications for healthcare and churches.
- Caller ID Restrictions: We block and suspend accounts using purchased DID's for Caller ID origination, ensuring only verified IDs are used (per FCC anti-spoofing rules). We use a web service <https://apilayer.com/> to check the age, provider, and type of DID used for the caller ID inserted by the customer. We do this each time before we allow scheduling of calls in our system.

Monitoring, Analytics, and Enforcement:

- Real-Time Call Pattern Analysis: We use AI-driven analytics to monitor for volume and message content BEFORE we allow scheduling of the calls.
- Post-Call Review: CDRs are audited daily for fraud signals; user reports of unwanted calls prompt immediate investigation and account holds.
- Traceback Commitment: We guarantee full response within 24 hours to traceback requests, providing logs, user data, and IP traces. In 2025, we've cooperated on 3 ITG requests without delay.

Training and Continuous Improvement:

- Staff training on FCC rules quarterly; annual audits by third-party compliance experts.

- Program updates based on FCC guidance, e.g., incorporating new threats like AI-generated deepfakes, while maintaining HIPAA compliance for healthcare clients.

Certification Statements:

- All originated calls are subject to this mitigation program, which takes reasonable steps to avoid illegal traffic. 47 CFR § 64.6304(a)
- We can not implement STIR/SHAKEN on any network portion due to not having control of the gateway dialing hardware and defer to the provider's signing certificate, resulting with a "B" rating for our outbound traffic.
- We currently validate DID's for ownership with a third party providing a call and speaking a code to the end user that is used to ensure that the DID is not being spoofed by a criminal pretending to be another organization.
- No prior certification removed by FCC and we have never been punished by the FCC for any infractions over the past 15+ years of servicing our relatively small customer base.

Date: September 28, 2025

Signature Thomas Mahoney

Thomas Mahoney, CEO Robotalker.com