

Robocall Mitigation Program – ThreePBX

1. Customer Vetting

ThreePBX requires all customers to submit valid and verifiable business credentials prior to account activation. This includes government-issued identification, business licenses, and EIN or corporate documentation. We carefully review all new applications to ensure they represent legitimate businesses with a valid need for voice services. Customers who cannot provide sufficient documentation or are deemed high-risk are rejected.

2. Traffic Monitoring & Controls

ThreePBX continuously monitors call traffic patterns to identify unusual activity, such as excessive short-duration calls, high-volume bursts, or other patterns consistent with unlawful robocalling. Automated detection systems are in place to generate alerts, which are reviewed by compliance staff. We enforce restrictions, implement call blocking, and suspend suspicious traffic when necessary. Customers proven to originate unlawful robocalls are immediately suspended or terminated.

3. Traceback & Enforcement Cooperation

ThreePBX actively participates in traceback efforts and cooperates fully with the Industry Traceback Group (ITG), the FCC, and law enforcement agencies. We commit to responding to traceback requests within 24 hours and provide full cooperation in investigations. Our compliance program includes record-keeping and internal escalation procedures to ensure rapid response. Repeat violators are permanently removed from our platform.

Certification Statement

ThreePBX affirms that it does not implement STIR/SHAKEN on its own network. Instead, we comply with FCC requirements through a robust Robocall Mitigation Program, as described above, to ensure that our services are not used to originate unlawful robocalls. This program reflects our ongoing commitment to protecting the integrity of communications and cooperating fully with regulatory requirements.