

Twiching General Trading PTE LTD

Robocall Mitigation Plan

Company Profile

Twiching General Trading is a foreign telecommunications service provider headquartered in Singapore, offering VoIP and interconnected voice services. Holding an Operating Company Number (OCN) license and STIR/SHAKEN compliance, the company serves a diverse international clientele while maintaining robust safeguards against illegal robocall traffic.

Commitment to Compliance

Twiching General Trading is fully committed to preventing the origination, transmission, or processing of illegal robocalls. This plan outlines specific reasonable steps taken to mitigate such traffic, in accordance with 47 CFR § 64.6305, including full cooperation with traceback and enforcement initiatives.

STIR/SHAKEN Implementation

Twiching General Trading has implemented the STIR/SHAKEN caller ID authentication framework on the IP portions of its network, consistent with its OCN license and FCC obligations under 47 CFR §§ 64.6301–64.6302. Partial implementation is certified, with authentication of unauthenticated SIP calls where feasible, and active progression toward full deployment across hybrid network segments. Non-IP portions apply equivalent measures, including caller ID validation and analytics-based filtering. Registration with the STIR/SHAKEN Policy Administrator has been completed, including acquisition of a Service Provider Code (SPC) token and generation of certificates for authentication. Attestation decisions are made internally, with optional third-party support for certificate management.

Network and Traffic Controls

- All IP interconnections are explicitly authorized, with defined routing permissions and class-of-service restrictions applied to each connection.
- Invalid, unallocated, spoofed, or malformed ANI/CLI is blocked in real time.
- Invalid outbound terminations are prohibited.
- Do Not Call (DNC) enforcement is enabled network-wide where applicable.
- Rate limiting and CLI reputation scoring are applied, particularly to new or high-volume customers.

Customer Vetting and Onboarding

- Mandatory signed service agreements include anti-robocall clauses and representations of legitimate usage.
- Comprehensive KYC requires business registration, government-issued identification, beneficial ownership disclosure (where applicable), operational website, and traffic use declaration.

- All submissions are verified against government databases and third-party sources.
- Customers are risk-classified (Low, Medium, High), with high-risk entities requiring management approval and enhanced monitoring.

Monitoring, Analytics, and Detection

- Advanced in-house analytics perform real-time pattern recognition, anomaly detection, and behavioral analysis.
- Daily reports identify spam indicators, suspicious patterns (e.g., high-volume short-duration calls, rapid ANI changes, sequential dialing), and flagged entities are investigated and blocked promptly.
- Call logs are maintained and reviewed regularly for excessive or anomalous activity.

Enforcement and Zero Tolerance

- Persistent violators are permanently blocked or terminated after investigation.
- Reseller customers must block downstream sources of illegal traffic.
- Immediate suspension or termination is authorized upon detection of abuse.

Traceback and Cooperation

- All traceback requests from the FCC, U.S. Telecom (Industry Traceback Consortium), law enforcement, or authorized entities are acknowledged and resolved within 24 hours.
- Full cooperation is provided, including traffic origin investigation, customer suspension during reviews, and permanent termination of confirmed violators.
- Records are retained to support investigations.

User Reporting

- User-friendly mechanisms encourage reporting of suspicious calls.
- Reports are investigated promptly, with decisive action against confirmed sources.

Ongoing Compliance and Updates

- Policies are reviewed annually or upon regulatory change.
- Regular staff training covers FCC rules, prevention techniques, and best practices.
- Customer education promotes responsible usage and awareness of consequences.
- Audits of traffic, protocols, and effectiveness are conducted routinely.