

I. Company Overview

Mission Security Technologies operates exclusively as a pure reseller of interconnected VoIP services to direct, local retail clients. We do not provide wholesale services, nor do we sell to downstream providers, carriers, or resellers. Mission Security Technologies does not own, operate, or maintain underlying network switching infrastructure or facilities. We rely entirely on our authorized upstream network providers to originate, terminate, and authenticate all voice traffic.

II. STIR/SHAKEN Compliance

Because Mission Security Technologies lacks its own network infrastructure to initiate, maintain, and terminate SIP calls, we do not directly generate STIR/SHAKEN SIP Identity headers. Instead, we rely entirely on our contracted upstream carrier(s) to apply STIR/SHAKEN call authentication on all calls originating on the network, consistent with FCC Caller ID Authentication Rules.

III. Upstream Provider Vetting and Management

Mission Security Technologies takes reasonable steps to ensure that the upstream VoIP providers we utilize are legitimate and compliant with federal telemarketing laws. We mandate that our underlying wholesale providers maintain up-to-date STIR/SHAKEN frameworks or Robocall Mitigation Plans as required by the FCC. We review upstream certifications to ensure they are listed and active in the [FCC Robocall Mitigation Database](#).

IV. Know-Your-Customer (KYC) Policies

To ensure our services are exclusively utilized for legitimate business operations, Mission Security Technologies enforces strict vetting policies for all prospective and existing end-user clients:

- **Direct Verification:** We require all clients to provide verifiable business information, including legal company name, physical address, federal tax ID (EIN), and authorized corporate officers.
- **Authorized Use Verification:** We require proof of authorization before enabling telephone numbers (e.g., matching customer details with Customer Service Records).

V. Monitoring, Suspicious Traffic, and Action

While Mission Security Technologies relies on upstream providers for core infrastructure, we proactively monitor our own end-user client activity to detect illegal robocalls:

- Usage Analysis: We monitor call detail records (CDRs) and review accounts exhibiting abnormal call volumes, unusually high short-duration calls, or suspicious calling patterns.
- Service Gating: Upon identifying suspicious activity or receiving abuse complaints, Mission Security Technologies immediately revokes outbound dialing privileges and investigates the offending client.

VI. Cooperation with Traceback and Law Enforcement

Mission Security Technologies pledges full cooperation with the FCC, state attorneys general, law enforcement authorities, and industry traceback consortia (e.g., USTelecom).

- We designate a specific 24/7 point of contact to receive and respond to formal traceback requests.
- Because all clients are direct retail users, we can instantly trace the origins of illegal robocalls to the specific offending customer and take immediate remedial action against bad actors.

VII. Enforcement and Blocking

In compliance with FCC directives, Mission Security Technologies will not accept or transmit voice traffic with U.S. NANP calling numbers from any upstream voice service provider that is not properly registered and active in the FCC Robocall Mitigation Database.