

Robocall Mitigation Program Description

Filer Name: Total Security Vision, Inc.

1. Overview:

Total Security Vision, Inc. has implemented a Robocall Mitigation Program consistent with **47 CFR § 64.6305(a)**. Because Total Security Vision does not have direct access to numbering resources from the North American Numbering Plan Administrator (NANPA) or Pooling Administrator and does not possess a Service Provider Code (SPC) token, the company qualifies for the STIR/SHAKEN exemption under **47 CFR § 64.6304(f)(2)**. As such, Total Security Vision has established proactive measures to prevent the origination of illegal robocall traffic.

2. Reasonable Steps Taken to Avoid Illegal Robocalls:

- **Customer Vetting:** Total Security Vision conducts a rigorous Know Your Customer (KYC) process for all clients, including identity verification, business registration checks, and a review of intended service use.
 - **Traffic Monitoring:** The company monitors call traffic for irregular patterns, including high call volumes, sequential dialing, and unusually short-duration calls that may indicate unlawful robocall activity.
 - **Contractual Controls:** All customer agreements explicitly prohibit illegal robocalling, with clear terms allowing immediate service suspension or termination for violations.
 - **Employee Training:** Staff members are trained to identify, flag, and escalate potential robocall traffic issues for immediate action.
-

3. Traceback Cooperation:

Total Security Vision is fully committed to **responding to traceback requests within 24 hours** from the Federal Communications Commission (FCC), law enforcement agencies, and the registered industry traceback consortium (USTelecom's Industry Traceback Group - ITG). The company cooperates actively in any investigations and enforcement efforts against suspected illegal robocallers.

4. Enforcement Actions:

Upon detection of illegal robocall activity:

- Services may be immediately suspended or terminated without prior notice.
 - Repeat violators are banned from service, and appropriate reports are made to regulatory and law enforcement bodies.
-

5. Certification Compliance:

Total Security Vision certifies that:

- It has not had any prior certification removed by Commission action;
 - It is not prohibited from filing in the Robocall Mitigation Database;
 - It has not implemented STIR/SHAKEN authentication on any portion of its network.
-

6. Additional Measures:

Total Security Vision periodically reviews and updates its robocall mitigation policies to adapt to emerging threats and to remain compliant with regulatory requirements.