

ROBOCALL MITIGATION PLAN

Provider Name: NetSecureIT Solutions

FRN (FCC Registration Number): 0038674206

Filing Date: 07/16/2026

1. Introduction & Operational Role

NetSecureIT Solutions is a non-facilities-based Voice Service Provider (VoIP reseller) offering white-label unified communications and voice services primarily to business and enterprise end-users.

Because NetSecureIT Solutions does not own, operate, or control physical switching infrastructure or Session Border Controllers (SBCs), it does not directly originate, transit, or terminate physical media streams, nor does it possess its own cryptographic STIR/SHAKEN signing certificates. Instead, NetSecureIT Solutions partners with premier, fully compliant, facility-based upstream wholesale carrier providers to route, sign, and terminate all customer traffic.

2. STIR/SHAKEN Implementation & Upstream Integration

Although NetSecureIT Solutions is non-facilities-based, we ensure full compliance with the FCC's caller ID authentication mandates through strict upstream carrier integration:

- **Upstream Compliance:** NetSecureIT Solutions exclusively utilizes upstream wholesale partners who are fully registered in the FCC's Robocall Mitigation Database (RMD) and have implemented STIR/SHAKEN across their networks.
 - **Attestation Coordination:** For numbers provisioned directly to our customers through our platform, we coordinate with our upstream partners to ensure that originating traffic receives **A-Level Attestation** (Full Attestation) wherever technically feasible.
 - **Customer-Provided Numbers:** For customers bringing their own telephone numbers, we verify the customer's "right to use" those numbers to ensure the traffic is appropriately authenticated and marked with the highest legally permissible attestation level by our upstream partners.
-

3. "Know Your Customer" (KYC) Onboarding Procedures

As a reseller holding the direct contractual and billing relationships with end-users, NetSecureIT Solutions implements robust "Know Your Customer" (KYC) protocols during customer onboarding to prevent bad actors from accessing our network. These procedures include:

- **Identity Verification:** We require all new business customers to provide their legal business name, physical corporate address, authorized point of contact, corporate registration/incorporation documents, and Tax ID/EIN. This information is cross-referenced against public state registries.
- **Traffic Profile Analysis:** During onboarding, customers must state their intended use case. We evaluate whether the customer intends to conduct conversational office calling, automated notifications, or high-volume outbound campaigns. High-volume outbound profiles are subjected to heightened regulatory and security scrutiny.
- **Verify Number Rights:** Customers must prove their right to use any Caller ID numbers not provisioned directly by NetSecureIT Solutions. This is done via Letters of Authorization (LOAs) or verified billing records from the original carrier. We strictly prohibit the spoofing of unassigned or unauthorized telephone numbers.

4. Network Monitoring & Traffic Abuse Detection

To ensure our platform is not used to originate illegal robocalls, NetSecureIT Solutions continuously monitors network usage metrics:

- **CDR Analysis:** We review Call Detail Records (CDRs) regularly to flag anomalous calling patterns, such as sudden, massive spikes in call volume, abnormally short average call duration (ACD), or exceptionally low call-completion rates (CCR).
- **Proactive Alerts:** We cooperate with automated security alerts and fraud-detection notifications generated by our upstream wholesale providers. If an upstream carrier flags traffic originating from one of our accounts, we immediately quarantine the traffic for review.

5. Explicit Commitment to Traceback Cooperation

NetSecureIT Solutions fully recognizes the critical role of traceback investigations in securing the telecom ecosystem.

- **Mandatory Cooperation:** NetSecureIT Solutions commits to fully cooperating with all traceback requests from the **Industry Traceback Group (ITG)**, the Federal Communications Commission (FCC), state Attorneys General, and federal law enforcement agencies.
- **24-Hour Response SLA:** We commit to responding to all official traceback inquiries **within 24 hours** of receipt.
- **Dedicated Response Contact:** We maintain a dedicated compliance contact and monitored email address to handle incoming traceback inquiries without delay:
 - **Contact Name/Title:** [Joseph T Nguyen / President]
 - **Contact Email:** [jnguyen@netsecureitsolutions.com]
 - **Contact Phone:** [562.888.1877 ext. 100]

6. Enforcement, Acceptable Use, and Service Termination

Our Terms of Service (ToS) and Acceptable Use Policy (AUP) explicitly prohibit the use of our services to originate, facilitate, or transmit illegal robocalls, spoofed caller IDs, or telemarketing fraud.

- **Account Suspension:** If NetSecureIT Solutions detects, or is notified by a traceback authority or upstream carrier, that a customer is originating unauthorized or illegal traffic, we will instantly suspend the offending trunk or account.
- **Permanent Termination:** If the customer cannot immediately demonstrate the legality of their traffic and right to use the transmitted Caller IDs, their services with NetSecureIT Solutions will be permanently terminated, and the customer will be blacklisted from re-establishing service.

Authorized Signature: _____



Joseph T Nguyen

President

NetSecureIT Solutions