

Robocall Mitigation Program Description

IT HUB Networks, Corp
VorTex VoIP Technology (DBA)

1. STIR/SHAKEN Implementation

IT HUB NETWORKS, Corp. is a small IP interconnected voice service provider dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. All outbound voice traffic is transmitted exclusively through the our upstream facilities-based carrier, Inteliquent, which performs STIR/SHAKEN authentication in compliance with 47 CFR §64.6301. IT HUB NETWORKS, Corp does not permit unsigned outbound traffic to the public switched telephone network (PSTN).

2. Customer Vetting and Know-Your-Customer (KYC) Procedures

The filer implements risk-based customer onboarding procedures including:

- Verification of legal business name and EIN
- Collection of physical business address
- Verification of website and public presence
- Confirmation of intended use of voice services
- Screening for high-risk verticals
- Review of caller ID usage legitimacy

High-risk accounts are subject to enhanced review and may be denied service.

3. Caller ID and Number Assignment Controls

The filer:

- Assigns telephone numbers only to verified customers
- Prohibits spoofing of unauthorized numbers
- Monitors caller ID consistency
- Immediately suspends accounts engaging in misleading or fraudulent caller ID usage

4. Traffic Monitoring and Analytics

The filer utilizes traffic monitoring tools and upstream carrier analytics to detect:

- High-volume short-duration calls
- Sequential dialing patterns
- Abnormal answer-seizure ratios
- Excessive call bursts
- Repeated complaints

Suspicious traffic is investigated and may result in immediate suspension.

5. Traceback Cooperation

The filer cooperates fully with traceback requests from:

- The Industry Traceback Group
- Upstream carriers
- Law enforcement

Records sufficient to identify the originating customer are maintained in accordance with FCC requirements.

6. Complaint Handling and Enforcement

Upon receiving complaints of suspected illegal robocalling:

- The filer investigates promptly
- Contacts the customer for explanation
- Suspends or terminates service if violations are confirmed
- Blocks traffic when necessary

7. Record Retention

Customer onboarding documentation and traffic records are retained for a commercially reasonable period sufficient to comply with traceback and regulatory requirements.

8. Ongoing Compliance

The filer reviews and updates its robocall mitigation policies as necessary to maintain compliance with evolving FCC rules and industry best practices.

9. Prohibited Traffic and Acceptable Use Policy

The filer does not provide services to robocall operators, mass autodialers, or entities engaged in illegal or high-risk automated calling campaigns.

The filer's services are intended exclusively for legitimate, user-generated voice communications initiated by verified customers. The filer does not knowingly provision services for:

- Unsolicited bulk robocalling
- Predictive dialer campaigns targeting consumers without consent
- Spoofed caller ID traffic
- Fraudulent or scam-related activity
- Artificial traffic pumping or traffic stimulation schemes

Customers are contractually prohibited from engaging in illegal robocalling activities. The filer monitors traffic patterns for indicators of non-user-generated or automated high-volume dialing behavior. Accounts found to be in violation are subject to immediate suspension or termination.