

iVoipe Inc. operates as a transit and wholesale telecommunications provider and does not originate voice calls to the United States Public Switched Telephone Network (PSTN). iVoipe does not assign, control, or manage U.S. NANP numbering resources and does not function as the originating voice service provider for U.S.-bound calls.

Although the iVoipe is exempt from STIR/SHAKEN implementation pursuant to 47 CFR § 64.6300(g), the company has implemented a comprehensive robocall mitigation program designed to prevent the transmission of illegal robocalls over its network.

1. Customer Onboarding Controls

iVoipe performs due diligence prior to onboarding customers, including:

- Know Your Customer (KYC) verification procedures
- Verification of business registration and corporate identity
- Review of service use case and traffic profile
- Contractual prohibitions against unlawful robocalling
- Requirement that customers comply with applicable U.S. and international telecommunications regulations

High-risk customers are subject to enhanced review prior to activation.

2. Traffic Monitoring and Analytics

iVoipe monitors network traffic patterns to detect suspicious activity, including:

- Abnormal call volume spikes
- Short-duration / high-volume traffic patterns
- Unusual Answer-Seizure Ratios (ASR)
- Invalid or spoofed CLI formats
- Traffic patterns inconsistent with declared customer use case

Automated monitoring tools and manual review processes are used to identify anomalous behavior.

3. Mitigation and Enforcement Actions

Upon detection of suspicious or potentially unlawful traffic, iVoipe may:

- Issue warnings or request clarification from the customer
- Temporarily suspend affected routes
- Block specific traffic streams
- Immediately terminate service for confirmed violations

iVoipe maintains internal escalation procedures to ensure rapid response to identified threats.

4. Traceback Cooperation

iVoipe cooperates with industry traceback efforts and responds promptly to requests from:

- U.S. regulators
- Upstream carriers
- Authorized traceback consortia

iVoipe maintains call detail records sufficient to trace traffic through its network and takes appropriate action when notified of illegal robocall activity.

5. Upstream and Downstream Controls

iVoipe works with reputable upstream and downstream partners and expects its counterparties to:

- Implement STIR/SHAKEN where required
- Maintain robocall mitigation programs
- Comply with FCC regulations and anti-robocall requirements

Traffic exchange agreements include compliance obligations related to unlawful robocalling.

iVoipe continuously reviews and updates its robocall mitigation practices to ensure compliance with applicable FCC requirements and industry best practices.