

Premier IT Networks Inc.

Robocall Mitigation Plan

Effective Date: August 18, 2026

1. Purpose

Premier IT Networks Inc. maintains this Robocall Mitigation Plan to help prevent its services from being used for illegal robocalls, caller-ID spoofing, fraud, or other unlawful calling activity.

2. Know Your Customer

Premier IT Networks verifies customers before providing voice services.

The company collects and reviews information such as:

- Customer legal/business name
- Business address
- Contact information
- Authorized customer representative
- Intended use of the voice service
- Expected calling volume

Customers may be subject to additional review when their calling activity appears unusual or presents a higher risk of illegal robocalling.

3. Customer Requirements

Customers are required to use Premier IT Networks services in compliance with applicable federal and state laws.

Customers may not use the service for:

- Illegal robocalls
- Fraudulent calling
- Unlawful caller-ID spoofing
- Other prohibited or illegal communications

Premier IT Networks may restrict, suspend, or terminate service when illegal or abusive calling activity is identified.

4. Upstream Providers

Premier IT Networks reviews its upstream voice providers and business partners and maintains appropriate contact information for those providers.

The company expects upstream providers to comply with applicable robocall mitigation and caller-ID requirements.

Premier IT Networks may take corrective action against an upstream provider associated with illegal or abusive traffic.

5. Traffic Monitoring

Premier IT Networks monitors voice traffic for unusual or suspicious activity.

Monitoring may include:

- Unusually high call volume
- Large numbers of short calls
- Rapid changes in calling activity
- Suspicious caller-ID activity
- Unusual calling patterns
- Customer complaints or traceback information

Suspicious activity may be investigated and appropriate action may be taken.

6. Blocking and Remediation

When Premier IT Networks identifies traffic that appears to be illegal or abusive, the company may:

- Investigate the activity
- Contact the customer or provider
- Block or restrict traffic
- Suspend the account
- Terminate the account or provider relationship

The action taken will depend on the nature and seriousness of the activity.

7. STIR/SHAKEN

Premier IT Networks will comply with applicable FCC STIR/SHAKEN requirements based on its role as a voice service provider.

Where STIR/SHAKEN applies, Premier IT Networks will use appropriate caller-ID authentication procedures and maintain the systems necessary to support compliance.

8. Traceback Cooperation

Premier IT Networks will cooperate with traceback requests from the FCC, law enforcement, and authorized traceback organizations.

Premier IT Networks commits to responding fully and within **24 hours** to applicable traceback requests.

The company will provide available information needed to identify the source of suspected illegal robocall traffic.

9. Recordkeeping

Premier IT Networks maintains appropriate records relating to:

- Customer verification
- Traffic investigations
- Blocking actions
- Complaints
- Traceback requests
- Robocall mitigation activities

10. Compliance Review

Premier IT Networks will periodically review this plan and update it when necessary to reflect changes in FCC requirements, the company's network, or its robocall mitigation procedures.

11. Responsible Contact

Robocall Mitigation Contact:

Name: Tzahi Zlikha

Title: President

Email: tzahiz@lhsip.com

Telephone: 914-276-5555

12. Company Certification

Premier IT Networks Inc. maintains this Robocall Mitigation Plan and will take reasonable steps to prevent its services from being used for illegal robocalls and unlawful caller-ID spoofing.

Premier IT Networks will cooperate with applicable regulatory and traceback investigations and will maintain accurate information in the FCC Robocall Mitigation Database as required.