

Robocall Mitigation Plan for Voipsecure Pty Ltd

About Voipsecure Pty Ltd

Voipsecure Pty Ltd ("Voipsecure") is a provider of mobile applications that facilitate voice communications. All inbound and outbound voice calls are processed through underlying providers that have fully implemented STIR/SHAKEN across their networks, ensuring that calls made on behalf of Voipsecure users are appropriately signed. Voipsecure does not provide direct API access or any other direct mechanism for users to interact with the underlying voice infrastructure.

STIR/SHAKEN Implementation Status

Voipsecure has not directly implemented STIR/SHAKEN as it does not qualify for an Operating Company Number (OCN). Due to this, Voipsecure is unable to obtain a Service Provider Code (SPC) token under the STI Governance Authority's SPC Token Access Policy. Consequently, Voipsecure qualifies for an extension from STIR/SHAKEN compliance obligations until such time as it becomes eligible for an SPC Token. However, Voipsecure relies on its upstream providers, all of whom have implemented STIR/SHAKEN, to sign calls originated on behalf of Voipsecure users.

Robocall Prevention and Mitigation Measures

Know Your Customer (KYC) Protocols

Voipsecure enforces strict KYC measures to prevent misuse of its services:

- Before a user can make a call, they must submit their **payment details** to **Google or Apple**. This includes providing a valid **credit card**, **mobile phone number**, and **email address** for verification.
- During the registration process, users must agree to Voipsecure's **Terms of Service**, which require them to maintain accurate and up-to-date account information.
- Users must either own the device they use with Voipsecure services or have explicit authorization from the device owner.
- The **Terms of Service** prohibit any use of the platform for fraudulent, deceptive, or illegal activities, including:
 - Transmission of unsolicited advertising, promotional content, or bulk commercial messages.
 - Caller ID spoofing, unauthorized multi-party calling, and misleading representations of identity.
 - Any activity that could expose Voipsecure to legal or regulatory liability.
- Users who become aware of prohibited use must report it immediately, and Voipsecure reserves the right to suspend or terminate accounts found in violation.

Know Your Upstream Provider Measures

Voipsecure does not accept third-party traffic beyond its own registered users. The platform works exclusively with a limited number of vetted VoIP providers, all of whom have implemented STIR/SHAKEN and comply with industry best practices.

- All outbound calls initiated through Voipsecure's application are routed

through these providers.

- There is no automated dialing, bulk dialing, or robocall capability within Voipsecure's system—calls must be manually initiated by users.

Traffic Monitoring and Mitigation

Voipsecure proactively monitors and mitigates abusive behavior on its platform:

- Automated systems analyze usage patterns to detect potential misuse, including:
 - Unusual call volume within a given period.
 - Repeated use of multiple devices under the same account.
 - Calling patterns that resemble known robocall tactics.
- If an account is flagged for suspicious activity, Voipsecure's telephony platform automatically blocks the user and suspends access.
- In addition to internal monitoring, Voipsecure collaborates with its upstream providers to utilize their analytics, monitoring, and mitigation tools to detect and address robocalls.

Traceback Cooperation

Voipsecure fully complies with traceback requests from regulatory authorities, law enforcement, and industry traceback initiatives.

- Upon receiving a traceback request, Voipsecure will respond within **24 hours** and cooperate fully in identifying and mitigating illegal robocalls originating from its platform.

Regulatory Compliance & Enforcement History

Within the past **two years**, neither Voipsecure nor any related entity under common ownership, management, or control has been the subject of any formal investigation or enforcement action concerning illegal robocalls, spoofing, or non-compliance with robocall mitigation regulations.