



Clark Access

Robocall Mitigation Program Description

1. Provider Identification and Role

Clark Access is a non-facilities-based, originating Voice over IP (VoIP) provider serving a limited number of business customers. The company currently supports approximately two customers with approximately fifteen endpoints in total. The company does not operate as an intermediate or transit provider.

2. STIR/SHAKEN Implementation

Clark Access does not directly implement STIR/SHAKEN authentication within its own network infrastructure. Instead, the company relies on its upstream carrier to perform STIR/SHAKEN authentication and call signing on its behalf. All outbound traffic is routed exclusively through this upstream provider, which is fully compliant with applicable STIR/SHAKEN requirements.

3. Customer Vetting and Know-Your-Customer (KYC)

All customers are manually vetted prior to service activation. The onboarding process includes verification of customer identity, confirmation of business purpose, and direct communication with customer representatives. No anonymous or automated account provisioning is permitted.

4. Traffic Monitoring and Analytics

The company actively monitors outbound call traffic for patterns consistent with illegal robocalling. Monitoring includes review of call volume, call duration, answer-seizure ratios, and dialing patterns. Due to the small scale of operations, both automated and manual review processes are used.

5. Use Case Restrictions

Services are limited to legitimate business and personal communications. The company prohibits autodialing campaigns, unlawful telemarketing, and any form of illegal robocalling. Customers are contractually required to comply with all applicable federal and state laws.

6. Mitigation and Enforcement Actions

If suspicious or non-compliant traffic is detected, the company will take immediate action, including temporary suspension of services, investigation of the customer, and termination of service if necessary. The company maintains the ability to rapidly disable any endpoint or account.

7. Traceback Cooperation

The company will respond promptly to traceback requests from regulators, law enforcement, and industry traceback organizations. The company commits to full cooperation in identifying and mitigating illegal robocall activity.

8. Network Architecture and Controls

The network is configured to prevent unauthorized call origination and restrict outbound calling to authenticated endpoints. The company does not allow open SIP relay or unauthenticated access. Logs are maintained to support traceback and investigation.

9. Ongoing Compliance

The company regularly reviews its policies and traffic to ensure continued compliance with applicable regulations. Given the limited customer base, the company maintains a high level of visibility and control over all traffic.