

Robocall Mitigation Plan

Provider Type:

Reseller of interconnected VoIP services. The company does not own or operate underlying transmission facilities and relies on upstream carriers for call routing and signaling.

1. STIR/SHAKEN Implementation Status

The provider does not have direct control over network infrastructure and therefore is not capable of independently implementing STIR/SHAKEN authentication.

The provider relies on its upstream carrier(s) to perform STIR/SHAKEN authentication and call signing where applicable.

2. Reliance on Upstream Providers

All outbound and inbound traffic is transmitted via contracted upstream voice service providers that:

- Are listed in the FCC Robocall Mitigation Database
- Have certified STIR/SHAKEN implementation or mitigation programs
- Are contractually required to comply with FCC robocall mitigation rules

The provider periodically verifies the RMD status of its upstream providers.

3. Know Your Customer (KYC) Procedures

The provider implements customer vetting procedures prior to service activation, including:

- Collection of customer identity information (legal name, address, contact details)
- Verification of business registration (for business customers)
- Review of intended use of services and traffic profiles
- Screening for high-risk categories (e.g., telemarketing, auto-dialing use cases)

Accounts deemed high-risk are subject to enhanced due diligence or may be denied service.

4. Traffic Monitoring and Analytics

The provider monitors customer traffic for suspicious patterns, including:

- Unusual call volumes or spikes
- High short-duration call ratios
- High complaint rates or traceback requests
- Sequential or invalid number dialing patterns

The provider may leverage upstream analytics tools and/or internal monitoring systems.

5. Complaint Handling and Traceback Cooperation

The provider:

- Maintains a process for receiving and responding to consumer complaints
 - Responds promptly to traceback requests from the Industry Traceback Group (ITG) and law enforcement
 - Investigates suspected illegal robocalling activity and takes appropriate action
-

6. Enforcement Actions

If a customer is suspected of illegal robocalling or spoofing, the provider will:

- Investigate the activity
- Require remediation or explanation
- Suspend or terminate service if violations are confirmed

Traffic may be blocked where necessary to prevent illegal activity.

7. Recordkeeping

The provider maintains records of:

- Customer onboarding and verification

- Traffic monitoring results
- Complaints and traceback responses

Records are retained in accordance with FCC requirements and internal policies.

8. Continuous Mitigation Efforts

The provider reviews and updates its robocall mitigation practices as necessary to remain compliant with FCC rules and industry best practices.

Certification:

The provider certifies that it has implemented the above robocall mitigation practices to prevent the origination and transmission of illegal robocalls.