

Robocall Mitigation Plan

Telimize, LLC

Role: Interconnected VoIP Provider

1. STIR/SHAKEN Implementation

Telimize, LLC, as an Interconnected VoIP service provider, has fully implemented the STIR/SHAKEN caller ID authentication framework across its entire IP voice network. Telimize confirms that implementation is complete and operational for all originated calls in accordance with FCC requirements.

2. Traceback Cooperation Commitment

Telimize, LLC commits to responding fully and in good faith within **24 hours** to all traceback requests from:

- The Federal Communications Commission (FCC)
- Law enforcement agencies
- The Industry Traceback Consortium

Telimize cooperates fully with these entities in investigating and stopping illegal robocallers that may attempt to use its network to originate calls.

3. Robocall Mitigation Database Certification

Telimize, LLC certifies that:

- It has not been prohibited from filing in the FCC Robocall Mitigation Database.
 - It is in full compliance with FCC robocall mitigation requirements applicable to Interconnected VoIP providers.
-

4. Regulatory & Enforcement History

Telimize, LLC further certifies that:

- It has not been subject to any Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
 - Within the prior two (2) years, neither Telimize, LLC nor any affiliated entity under common ownership, management, directors, or control has been subject to any formal Commission, law enforcement, or regulatory action with findings of actual or suspected wrongdoing related to transmitting, encouraging, assisting, or facilitating illegal robocalls or caller ID spoofing.
-

5. Robocall & Fraud Mitigation Practices

Telimize maintains a comprehensive robocall mitigation framework using advanced third-party and in-house monitoring solutions.

A. Dynamic Fraud Detection & Call Pattern Analysis

Telimize utilizes a third-party SIP fraud prevention platform that:

- Performs dynamic fraud analysis prior to call setup
- Automatically learns traffic patterns per subscriber, trunk, and destination
- Detects and prevents fraud attacks in milliseconds
- Blocks suspicious outbound robocall attempts
- Prevents unauthorized use of the telephone network

Legitimate calls continue uninterrupted while fraudulent or suspicious traffic is mitigated in real time.

B. Real-Time Traffic Monitoring & Blocking Controls

Telimize's security infrastructure prevents robocalls and TDoS attacks through:

- On-net call screening from external networks by Calling SPID/OCN

- Calling number or prefix validation
- Shield databases of invalid and high-risk numbers
- Blocking numbers with poor reputation scoring

The system performs real-time traffic analysis and can:

- Block suspected robocalls
- Divert calls to voicemail
- Divert calls to CAPTCHA verification systems requiring human interaction

C. Network Operations & Fraud Monitoring

Telimize operates a 24/7 Network Operations Center (NOC) that:

- Continuously monitors network traffic
- Identifies suspicious call patterns
- Reviews abnormal user behavior
- Investigates customer-reported issues

Additionally, a dedicated Fraud Monitoring Team works around the clock to detect unusual account activity or illegal misuse of services.

D. Caller ID Authentication & Anti-Spoofing Controls

Telimize, LLC uses advanced anti-spoofing technology to prevent caller ID manipulation. Customers are not permitted to arbitrarily alter caller ID information on outbound calls originating from Telimize services. All outbound caller ID information must comply with authentication and verification policies.