

ROBOCALL MITIGATION AND STIR/SHAKEN POLICY

Company: Goloo Tech LLC

FCC Registration Number (FRN): 0037896065

Date of Implementation: 01.01.2026

Policy Version: 1.0

1. PURPOSE AND SCOPE

Goloo Tech LLC ("Company," "we," "our," or "us") is committed to combatting illegal robocalls and call spoofing as a gateway provider in accordance with the Federal Communications Commission's ("FCC") rules implementing the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. This Robocall Mitigation and STIR/SHAKEN Policy ("Policy") outlines our comprehensive framework to authenticate, mitigate, and prevent illegal robocall traffic originating from, or transiting through, our network.

This Policy applies to all voice traffic carried by Goloo Tech LLC, including traffic from downstream providers, enterprise customers, and any other entities utilizing our network for voice service origination or termination.

2. STIR/SHAKEN IMPLEMENTATION

2.1 Full Implementation Status

Goloo Tech LLC has fully implemented the STIR/SHAKEN framework across our entire IP-based network. We possess our own secure key infrastructure and are a registered participant in the industry's certificate governance system.

2.2 Authentication Practices

- **Originating Traffic:** For all SIP calls originated on our network, we apply the highest appropriate attestation level:
 - **Full Attestation (A):** Applied when we are the originating service provider, have a direct authenticated relationship with the caller, and have established the caller's right to use the calling number.
 - **Partial Attestation (B):** Applied when we are the originating service provider but cannot fully verify the caller's right to use the calling number (e.g., for certain enterprise customers with complex numbering arrangements).

- **Gateway Attestation (C):** Applied when we act as a gateway provider for traffic entering the U.S. telephone network from international or non-IP networks.
- **Terminating Traffic:** We verify and validate STIR/SHAKEN signatures on all authenticated calls we receive and preserve verification results throughout call processing.

2.3 Governance and Certificate Management

We maintain a robust certificate management system, including:

- Secure storage of private signing keys
 - Regular certificate renewal and revocation processes
 - Compliance with certificate authority requirements
 - Audit trails for all signing activities
-

3. ROBOCALL MITIGATION PROGRAM

3.1 Know Your Customer (KYC) Procedures

Before accepting any customer traffic, Goloo Tech LLC conducts thorough due diligence:

- Verification of business registration and physical address
- Collection of valid contact information for at least two representatives
- Assessment of the customer's business type and expected call patterns
- Review of the customer's own robocall mitigation practices for downstream providers
- Execution of legally binding agreements prohibiting illegal robocalling and requiring compliance with all applicable laws

3.2 Ongoing Monitoring and Analysis

We employ a multi-layered monitoring system:

- **Real-time Analytics:** AI-driven analysis of call patterns, including call frequency, duration, destination patterns, and answer rates
- **Anomaly Detection:** Automated systems flag unusual spikes in traffic volume or patterns inconsistent with historical data
- **Reputation Monitoring:** Integration with industry-wide call analytics and reputation services

- **Signature Analysis:** Monitoring of attestation levels and verification failures

3.3 Mitigation Actions and Traffic Blocking

Upon detection of suspected illegal robocall traffic:

1. **Immediate Investigation:** Our security team investigates flagged traffic within 15 minutes of detection
2. **Progressive Actions:** We may implement, in escalating order:
 - Rate limiting of suspicious traffic
 - Request for additional customer validation
 - Temporary suspension of specific routes or customers
 - Permanent termination of service for confirmed bad actors
3. **Blocking Criteria:** We block traffic that:
 - Shows clear patterns consistent with IRSF (International Revenue Share Fraud)
 - Originates from unauthorized or spoofed numbers
 - Generates consistent consumer complaints
 - Is identified as malicious by industry traceback entities

3.4 Traceback Cooperation

Goloo Tech LLC maintains 24/7/365 availability to respond to traceback requests from:

- The Industry Traceback Consortium (ITC)
- U.S. Law Enforcement
- Regulatory agencies
- Other registered providers

Designated Traceback Contact:

Name: Tanveer Javaid

Title: Chief Compliance Officer

Email: support@golootech.com

We commit to responding to valid traceback requests within 2 hours and providing complete, accurate information about the source of suspected illegal calls.

4. UNACCEPTABLE USES AND PROHIBITED ACTIVITIES

The following activities are strictly prohibited on our network:

- **Spoofing:** Transmission of misleading or inaccurate caller ID information
- **Illegal Robocalling:** Calls made without prior express consent where required by law
- **Call Flooding:** Excessive call volumes intended to disrupt called parties or networks
- **Wangiri/Fraudulent Calls:** One-ring scams or other fraudulent calling schemes
- **Harassment:** Calls intended to harass, threaten, or intimidate called parties
- **Violation of DNC:** Calls to numbers on the National Do Not Call Registry (where applicable)

5. COMPLIANCE WITH FCC RULES AND FILINGS

5.1 FCC Robocall Mitigation Database

Goloo Tech LLC has filed the required certification in the FCC's Robocall Mitigation Database, confirming our implementation of STIR/SHAKEN and our robocall mitigation program. We will promptly update this filing if our mitigation practices materially change.

5.2 Interconnection Requirements

In accordance with FCC rules, we will:

- Not accept traffic from intermediate or voice service providers not listed in the Robocall Mitigation Database
- Cease accepting traffic from any provider whose filing is removed from the Database
- Take steps to ensure our downstream providers are also properly registered

5.3 Recordkeeping and Reporting

We maintain detailed records for a minimum of two years, including:

- All customer agreements and KYC documentation
- Call detail records (CDRs) with authentication/verification data
- Monitoring alerts and mitigation actions taken

- Traceback requests and responses
 - Consumer complaints and resolutions
-

6. TRAINING AND AWARENESS

- **Employee Training:** All relevant personnel receive annual training on robocall mitigation requirements, STIR/SHAKEN operations, and traceback procedures.
 - **Customer Education:** We provide resources to customers about legal calling practices and require them to pass similar requirements to their downstream users.
 - **Industry Participation:** We actively participate in industry forums (e.g., ATIS, SIP Forum) to stay current with evolving best practices.
-

7. POLICY REVIEW AND UPDATES

This Policy will be reviewed at least annually and updated as necessary to reflect:

- Changes in FCC regulations
 - Evolving industry standards
 - Technological advancements
 - Lessons learned from mitigation activities
-

8. ACKNOWLEDGMENT

This Policy has been reviewed and approved by Goloo Tech LLC's executive management and legal counsel. We affirm our commitment to being a responsible gateway provider and partner in the industry-wide effort to eliminate illegal robocalls.

Approved By:

Ali Haider
Chief Executive Officer
Goloo Tech LLC

Tanveer Javaid
Chief Compliance Officer
Goloo Tech LLC