

Robocall Mitigation Plan

SipSmart, LLC

Updated for FCC Robocall Mitigation Database Compliance – 2026

1. Purpose

SipSmart, LLC ("SipSmart") is committed to preventing illegal robocalls, caller ID spoofing, and fraudulent telecommunications traffic from originating on or transiting through its network.

SipSmart complies with 47 CFR § 64.6305 and has established reasonable and proactive mitigation procedures designed to prevent the origination and transmission of unlawful robocalls, including for traffic not authenticated using STIR/SHAKEN.

2. Network Overview

SipSmart operates an IP-based telecommunications network providing services including:

- SIP voice origination
- SIP voice termination
- Telephone number provisioning
- SIP trunking
- Programmable Voice APIs
- Voice routing and transit services
- LRN lookup and number intelligence services
- Related telecommunications services

SipSmart provides services to business customers and authorized resellers and does not originate calls on its own behalf.

3. STIR/SHAKEN Implementation

SipSmart implements STIR/SHAKEN authentication in the IP portions of its network where technically feasible and where SipSmart has a direct authenticated relationship with the originating customer.

SipSmart validates caller identity before assigning attestation and does not knowingly attest calls presenting unauthorized or misleading caller identification.

For traffic not authenticated using STIR/SHAKEN, SipSmart applies the mitigation measures described in this Plan.

4. Customer Vetting & Risk Assessment

Before activating service, SipSmart performs customer onboarding procedures that include collecting and reviewing:

- Legal business name
- Business address
- Contact information
- Nature of business
- Intended use of telecommunications services

SipSmart evaluates customer risk based upon the proposed use of its services and may request additional documentation where elevated risk indicators are identified.

SipSmart reserves the right to delay, deny, suspend, or terminate service where compliance concerns exist.

5. Caller ID Authorization

Customers may originate traffic only using:

- Telephone numbers assigned by SipSmart;
- Telephone numbers obtained through authorized upstream providers; or
- Telephone numbers the customer demonstrates authorization to use.

SipSmart maintains records of numbers assigned through its platform and validates caller ID authorization prior to assigning STIR/SHAKEN attestation where applicable.

SipSmart may block or reject calls presenting invalid, misleading, or unauthorized caller identification.

6. Traffic Monitoring & Preventative Mitigation

SipSmart employs reasonable mitigation procedures designed to identify potentially unlawful calling activity.

Monitoring includes review of:

- Call volume anomalies
- Sudden traffic spikes
- High short-duration call ratios
- Invalid or unauthorized ANI usage
- Traffic inconsistent with the customer's stated business purpose
- Customer complaint trends
- Internal CDR analysis

Where elevated risk is identified, SipSmart may temporarily restrict traffic, require additional documentation, or suspend service pending investigation.

7. Response to Suspected Illegal Activity

If SipSmart identifies or is notified of suspected illegal robocalling or caller ID spoofing, SipSmart may immediately:

- Suspend customer traffic
- Block specific caller IDs
- Restrict routing
- Disable accounts
- Terminate service agreements
- Initiate traceback inquiries

SipSmart takes mitigation measures promptly to prevent continued transmission of potentially unlawful traffic.

8. Traceback Cooperation

SipSmart cooperates with:

- The USTelecom Industry Traceback Group (ITG)
- The Federal Communications Commission
- Law enforcement agencies
- Authorized upstream and downstream service providers

SipSmart responds promptly to traceback requests and provides available call detail information and customer records as required.

Customers are contractually required to cooperate with traceback investigations.

9. Do Not Originate (DNO) & Data-Based Blocking

SipSmart subscribes to and implements the USTelecom Industry Traceback Group Do Not Originate (DNO) list and blocks numbers identified on that list where administratively and technically feasible.

SipSmart also reviews publicly available FCC and FTC complaint information as part of its ongoing compliance efforts.

Where complaint data, traceback information, or internal monitoring indicates elevated risk, SipSmart may:

- Block destination numbers
- Block source ANIs
- Restrict routing
- Suspend customer traffic pending investigation

SipSmart uses internal call detail record analysis to identify and mitigate suspicious calling patterns.

10. Foreign-Originated Traffic

To the extent SipSmart receives traffic from foreign-based customers or providers for delivery into the United States, SipSmart applies the mitigation procedures described in this Plan prior to routing such traffic into the U.S. PSTN.

SipSmart may block or suspend foreign-originated traffic presenting indicators of illegal robocalling and will comply promptly with FCC directives requiring blocking or mitigation of unlawful international traffic.

11. Mitigation for Non-STIR/SHAKEN Traffic

For traffic not authenticated using STIR/SHAKEN, SipSmart relies upon:

- Customer identity verification
- Caller ID authorization procedures

- Traffic monitoring
- DNO implementation
- Internal CDR analysis
- Immediate suspension authority
- Traceback cooperation

These measures constitute SipSmart's reasonable robocall mitigation efforts.

12. Record Retention

SipSmart maintains customer identification information, call detail records, STIR/SHAKEN-related records (where applicable), and compliance documentation for a commercially reasonable period consistent with business operations and applicable regulatory requirements.

13. Ongoing Review

SipSmart periodically reviews and updates its robocall mitigation procedures to remain aligned with evolving FCC regulations, industry best practices, and emerging threats.