

Robocall Mitigation Plan

Smart Automation Systems SAS

2026 Update – FCC Robocall Mitigation Database

1. Purpose

Smart Automation Systems SAS (“SAS”) is a Colombian corporation providing communications software and routing services to business customers.

SAS is committed to preventing illegal robocalls and caller ID spoofing from being transmitted through its platform to recipients in the United States.

SAS maintains a robocall mitigation program designed to implement reasonable steps to prevent the origination and transmission of unlawful robocalls consistent with applicable FCC requirements for foreign-originating providers.

2. Business Model & Network Role

SAS provides cloud-based communications software and call routing services to business customers.

SAS:

- Does not operate a U.S. PSTN network
- Does not assign U.S. telephone numbers
- Does not manage U.S. numbering resources
- Does not directly interconnect with U.S. terminating carriers

Calls destined for the United States are delivered to a contracted U.S.-based telecommunications provider for routing into the U.S. PSTN.

SAS functions as a foreign-originating provider.

3. Customer Vetting & Risk Assessment

Prior to activation of service, SAS:

- Collects legal business name and registration information
- Verifies contact details
- Reviews the customer’s business model

- Evaluates intended calling use case

SAS may request additional documentation where elevated risk indicators are identified.

SAS reserves the right to delay, deny, or condition activation of service based on compliance risk assessment.

4. Contractual Compliance Requirements

SAS contractually requires customers placing calls to U.S. recipients to comply with:

- The Telephone Consumer Protection Act (TCPA)
- The Truth in Caller ID Act
- FCC robocall mitigation rules
- Applicable federal and state telemarketing laws

Customers are responsible for obtaining legally required consumer consent.

Customer agreements require cooperation with regulatory inquiries and traceback investigations.

Failure to comply constitutes grounds for immediate suspension or termination.

5. Caller ID Controls

SAS requires customers to use only telephone numbers they are legally authorized to use.

SAS does not permit:

- Misleading caller ID
- Unauthorized number use
- Intentional spoofing

If suspicious caller ID behavior is detected, SAS may:

- Restrict traffic
- Require documentation
- Suspend the customer account

6. Traffic Monitoring & Preventative Measures

SAS implements reasonable mitigation measures designed to prevent unlawful robocalling activity, including:

- Monitoring call volume patterns
- Identifying sudden traffic spikes
- Reviewing high short-duration call ratios
- Comparing traffic behavior to the customer's stated business purpose

Where anomalies are detected, SAS may:

- Temporarily restrict traffic
- Request supporting documentation
- Suspend or terminate service pending investigation

SAS applies these measures proactively and not solely in response to complaints.

7. Response to Suspected Illegal Activity

If SAS identifies or is notified of suspected illegal robocalling activity, SAS may:

- Immediately suspend traffic
- Disable customer accounts
- Block specific source identifiers
- Terminate service agreements

SAS takes mitigation action promptly to prevent continued transmission of potentially unlawful traffic.

8. Traceback Cooperation

SAS cooperates with:

- U.S.-based telecommunications providers
- The USTelecom Industry Traceback Group (ITG)
- The FCC
- Law enforcement authorities

Upon request, SAS will provide relevant information regarding originating customers and assist in traceback investigations.

SAS requires its customers to cooperate fully in such investigations.

9. Mitigation for Traffic Destined to the United States

For traffic routed to the United States, SAS relies on:

- Customer identity verification
- Contractual compliance requirements
- Caller ID authorization controls
- Traffic monitoring and anomaly detection
- Immediate suspension authority
- Cooperation with U.S. gateway providers

These measures constitute SAS's reasonable mitigation efforts as a foreign-originating provider.

10. Record Retention

SAS retains:

- Customer identification information
- Call detail metadata
- Compliance-related communications

For a commercially reasonable period consistent with operational and regulatory needs.

11. Ongoing Review

SAS periodically reviews and updates its mitigation procedures to remain aligned with evolving FCC guidance and industry best practices.