

Robocall Mitigation Plan

Provider Information

Provider Name: AW Core Services LLC

FCC Registration Number (FRN): 0037702644

Service Type: Interconnected VoIP

Date Implemented: 01/01/2026

1. Purpose and Scope

AW Core Services LLC is committed to preventing illegal robocalls and protecting the integrity of the U.S. telecommunications network. This Robocall Mitigation Plan describes the policies, procedures, and technical measures implemented to mitigate the origination and transmission of unlawful robocalls, including spoofed and fraudulent calls, in compliance with FCC rules, the TRACED Act, and applicable industry best practices.

This plan applies to all voice traffic originated, terminated, or transited through AW Core Services LLC's network.

2. STIR/SHAKEN Status

AW Core Services LLC has implemented STIR/SHAKEN authentication for SIP-based voice traffic to the extent technically feasible.

- **Authentication:** We authenticate outbound calls using STIR/SHAKEN where required.
 - **Verification:** We verify inbound STIR/SHAKEN attestation levels when receiving calls from upstream providers.
 - **Non-IP or Unsupported Traffic:** For traffic that cannot support STIR/SHAKEN, we apply additional robocall mitigation measures as described below.
-

3. Know Your Customer (KYC) and Onboarding Controls

To prevent bad actors from accessing our network, we apply strict customer vetting procedures, including:

- Verification of customer identity (legal name, business address, contact information)
- Validation of business purpose for voice services

- Collection of supporting documentation (business registration, EIN/Tax ID, website, use case)
- Risk assessment for high-volume or outbound-only calling customers
- Enhanced due diligence for international or high-risk traffic profiles

Customers are prohibited by contract from engaging in illegal robocalling, spoofing, or fraudulent activity.

4. Traffic Monitoring and Analytics

AW Core Services LLC actively monitors voice traffic for indicators of illegal or suspicious activity, including but not limited to:

- High call volumes or burst patterns
- Short call durations
- High answer-to-seizure ratios (ASR anomalies)
- Repeated calling to invalid or unassigned numbers
- Consumer complaints or traceback notifications

Automated and manual reviews are conducted on a continuous basis.

5. Blocking, Mitigation, and Enforcement Actions

When suspicious or illegal robocall activity is detected, AW Core Services LLC takes prompt mitigation actions, including:

- Immediate call blocking or rate limiting
- Suspension or termination of customer accounts
- Removal of affected telephone numbers
- Notification to upstream or downstream providers
- Cooperation with traceback requests from the Industry Traceback Group (ITG)

Repeat or egregious violations result in permanent service termination.

6. Handling of Spoofed and Invalid Caller ID

AW Core Services LLC prohibits the use of spoofed or misleading caller ID information except where legally permitted (e.g., authorized business use).

We actively block calls with:

- Invalid, unassigned, or unallocated NANP numbers
 - Caller IDs on the FCC Do-Not-Originate (DNO) list
 - Known fraudulent or abusive numbers
-

7. Complaint Handling and Traceback Cooperation

We maintain procedures to receive, investigate, and respond to robocall complaints from consumers, regulators, and industry partners.

- Dedicated compliance contact: areeb@awcoreservices.com
 - Timely response to ITG and FCC traceback requests
 - Preservation of call detail records (CDRs) as required by law
-

8. Recordkeeping and Continuous Improvement

AW Core Services LLC retains relevant records related to robocall mitigation, including customer onboarding data, traffic monitoring logs, and enforcement actions.

We regularly review and update our robocall mitigation practices to address emerging threats, regulatory changes, and industry guidance.