

Robocall Mitigation Plan

Alpine Valley Consulting, LLC

2026 Update – FCC Robocall Mitigation Database

1. Purpose

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

AVC maintains a robocall mitigation program designed to implement reasonable and proactive measures to prevent the origination and transmission of unlawful robocalls in accordance with applicable FCC rules, including 47 CFR § 64.6305, and applies mitigation procedures for traffic that is not authenticated using STIR/SHAKEN.

2. Business Model & Network Role

AVC operates an IP-based telecommunications network providing services to business customers, including:

- SIP voice origination
- SIP voice termination
- Telephone number provisioning
- SIP trunking
- Voice routing and transit services

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

To the extent AVC receives traffic from foreign-originating providers for delivery into the United States, AVC functions as a gateway provider under applicable FCC rules.

3. Customer Vetting & Risk Assessment

Prior to activation of service, AVC performs customer due diligence, including:

- Collecting legal business name and registration information
- Verifying business contact information

- Reviewing the customer's business model
- Evaluating the intended use of telecommunications services
- Assessing potential compliance risks based on available information

Where elevated compliance risks are identified, AVC may request additional documentation before activating service.

AVC reserves the right to delay, deny, suspend, or terminate service based on its compliance risk assessment.

4. Contractual Compliance Requirements

AVC contractually requires its customers to comply with all applicable telecommunications laws and regulations, including but not limited to:

- The Telephone Consumer Protection Act (TCPA)
- The Truth in Caller ID Act
- FCC Robocall Mitigation requirements
- STIR/SHAKEN obligations where applicable
- Applicable federal and state telemarketing laws

Customers are responsible for obtaining all legally required consumer consents before placing calls.

Customer agreements require cooperation with regulatory inquiries and traceback investigations.

Failure to comply with these obligations constitutes grounds for immediate suspension or termination of service.

5. Caller ID Controls

Customers may transmit calls only using:

- Telephone numbers assigned by AVC; or
- Telephone numbers the customer is legally authorized to use.

AVC maintains records of numbers assigned through its network and validates caller ID authorization before assigning STIR/SHAKEN attestation where applicable.

AVC does not permit:

- Misleading caller identification
- Unauthorized telephone number usage
- Intentional caller ID spoofing

If suspicious caller ID activity is detected, AVC may:

- Restrict traffic
 - Request supporting documentation
 - Block specific caller IDs
 - Suspend customer accounts
-

6. Traffic Monitoring & Preventative Measures

AVC implements reasonable mitigation measures designed to identify and prevent unlawful robocalling activity.

These measures include monitoring for:

- Unusual call volume patterns
- Sudden traffic spikes
- High short-duration call ratios
- Invalid or unauthorized ANI usage
- Traffic inconsistent with the customer's stated business purpose
- Other indicators of potentially unlawful calling activity identified through internal call detail record (CDR) analysis

Where anomalies are detected, AVC may:

- Temporarily restrict traffic
- Require additional documentation
- Suspend or terminate service pending investigation

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

7. Response to Suspected Illegal Activity

If AVC identifies or is notified of suspected illegal robocalling activity, receives a traceback request, or otherwise determines that traffic presents a significant compliance risk, AVC may immediately:

- Suspend customer traffic
- Disable customer accounts
- Block specific caller IDs or source identifiers
- Restrict routing
- Request supporting documentation
- Terminate service agreements

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

8. Traceback Cooperation

AVC cooperates fully with:

- The USTelecom Industry Traceback Group (ITG)
- The Federal Communications Commission (FCC)
- Federal, state, and local law enforcement agencies
- Authorized upstream and downstream telecommunications providers

Upon receipt of a traceback request from the ITG, the FCC, a law enforcement agency, or an authorized telecommunications provider, AVC will acknowledge the request promptly and will make commercially reasonable efforts to provide all available information necessary to assist the investigation.

AVC is committed to responding to traceback requests within twenty-four (24) hours of receipt whenever reasonably practicable and prioritizes such requests to ensure timely cooperation.

AVC requires its customers to cooperate fully in traceback investigations and to provide information necessary to facilitate a timely response.

Failure to cooperate may result in immediate suspension or termination of service.

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

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

In addition, AVC reviews publicly available FCC and FTC complaint information as part of its ongoing compliance and risk assessment procedures.

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

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

AVC also utilizes internal call detail record (CDR) analysis to identify suspicious calling patterns and source ANIs associated with potentially unlawful activity.

10. Foreign-Originated Traffic

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

AVC 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, AVC relies on:

- Customer identity verification
- Caller ID authorization procedures
- Traffic monitoring and anomaly detection
- Implementation of the ITG Do Not Originate (DNO) list
- Internal CDR analysis
- Immediate suspension authority
- Cooperation with traceback investigations

These measures constitute AVC's reasonable robocall mitigation efforts for non-authenticated traffic.

12. Record Retention

AVC retains:

- Customer identification information
- Call detail records (CDRs)
- STIR/SHAKEN-related records where applicable
- Traceback correspondence
- Compliance-related communications

for a commercially reasonable period consistent with operational requirements and applicable regulatory obligations.

13. Regulatory Compliance Contact

AVC maintains designated personnel responsible for robocall mitigation and regulatory compliance.

Regulatory notices, traceback requests, law enforcement inquiries, and carrier compliance requests are monitored and prioritized to facilitate responses within the timeframes described in this Plan.

14. Ongoing Review

AVC periodically reviews and updates this Robocall Mitigation Plan to remain aligned with evolving FCC regulations, industry best practices, traceback requirements, and emerging threats.

AVC is committed to maintaining a robust compliance program and implementing reasonable measures designed to prevent the origination and transmission of illegal robocalls while cooperating fully with industry partners and regulatory authorities.