

AspenView Network Solutions

Robocall Mitigation Plan

STIR/SHAKEN Implementation & Robocall Mitigation Database (RMD) Certification Support

Company Overview

AspenView Network Solutions (“AspenView” or “Company”) is a provider of voice and network services to commercial and carrier markets. AspenView’s network and service offerings are designed to support scalable, secure communications and interoperability across interconnected voice networks.

1) Robocall Mitigation Measures

AspenView maintains and enforces reasonable practices designed to prevent its network from being used to originate, transmit, or terminate illegal robocall traffic. The Company’s program includes:

- Customer onboarding and verification controls (KYC/KYB)
 - Traffic monitoring and anomaly detection
 - Enforcement actions and escalation procedures
 - Rapid response to traceback and law enforcement inquiries
-

2) Traceback Cooperation & Response Commitment

Commitment

AspenView commits to responding to traceback requests from:

- The FCC,
- Federal/State law enforcement, and
- The Industry Traceback Consortium (ITC) / Industry Traceback Group (as applicable),

within 24 hours of receipt, and to cooperate in good faith with investigations into suspected unlawful robocall activity.

Escalation & Remediation

When suspicious traffic patterns are detected, AspenView may take one or more of the following actions based on risk and evidence:

- Open a compliance case and require customer explanation and supporting records
 - Implement traffic restrictions, including temporary blocks as warranted
 - Suspend or terminate service for non-compliant or high-risk activity
 - Preserve relevant logs where required or appropriate for investigations
-

3) Traceback Contact Information

Name: Benjamin Pearson

Title: Designated Robocall Mitigation / Traceback Contact

Email: *(add official email address here)*

Phone: 1 866 312 8662

(Note: RMDB filings typically expect a monitored email inbox used specifically for traceback requests.)

4) Traffic Monitoring, Call Analytics & Blocking

AspenView employs call analytics and monitoring controls intended to detect and mitigate suspicious or unlawful calling behaviors. These controls may include, as applicable to the service type:

- Pattern and volume/velocity monitoring (e.g., short-duration bursts, high ASR/low ACD anomalies)
- Detection of invalid, unallocated, or prohibited calling patterns
- Review workflows for flagged traffic and customer activity
- Blocking or throttling mechanisms when traffic meets predefined risk thresholds
- Ongoing review of upstream/downstream interconnection partners for compliance posture

Emergency Services Protection

AspenView does not intentionally block calls to **911**, PSAPs, or other government-designated emergency numbers.

5) Know Your Customer (KYC/KYB) Program

AspenView maintains customer due diligence practices designed to deter illicit robocall operations and reduce risk exposure.

Customer Information Collected (Illustrative)

- Legal entity name and any DBA(s)
- Business address and billing address
- Formation/incorporation documentation (where applicable)
- Tax identifier (EIN/FTIN or equivalent)
- Authorized user/contact details
- Description of intended use case and dialing/traffic profile

Verification Methods (Illustrative)

- Identity verification for principals/authorized signers (government-issued ID where legally appropriate)
- Business verification documentation (e.g., formation documents, utility bill, proof of address)
- Validation of payment method and billing controls
- Additional vetting for higher-risk use cases (lead gen, outbound, high-volume campaigns)

Risk-Based Monitoring

Customers or use cases classified as elevated risk may be subject to:

- Additional documentation requirements
- Higher frequency reviews and monitoring
- Pre-approval of traffic profiles and calling campaigns
- Mandatory opt-in/consent evidence retention (where applicable)

6) Validating the Right to Use Telephone Numbers

AspenView requires that customers only originate calls using telephone numbers that are properly assigned, provisioned, or ported through compliant processes.

Controls may include:

- Inventory tracking for numbers assigned by AspenView
 - Documentation and validation for customer-provided/porting numbers
 - Review of number authorization when anomalies or disputes arise
-

7) Accepting Traffic from Other Providers

AspenView maintains interconnection policies intended to reduce exposure to illegal traffic. Depending on network role, AspenView may:

- Accept traffic only from providers that appear in the FCC RMD and are not subject to delisting actions, as applicable
 - Apply heightened scrutiny for gateway pathways and foreign-originating call routes
 - Require contractual commitments regarding lawful traffic and traceback cooperation
-

8) STIR/SHAKEN Authentication & Verification (As Applicable)

AspenView's STIR/SHAKEN practices depend on the Company's role in the call path and the technical feasibility for particular traffic types.

- **When operating as an originating Voice Service Provider:** AspenView applies STIR/SHAKEN caller ID authentication to calls for which it is the appropriate signer, consistent with FCC requirements and industry standards.
- **When operating as a Gateway or Intermediate Provider:** AspenView performs verification of STIR/SHAKEN identity headers when present and applies additional analytics/controls for unsigned or non-verified traffic, consistent with applicable obligations.

(Insert: the specific STI-PA/CA vendor(s), signing/verification approach, attestation policy, and any exemptions or non-IP handling AspenView actually uses.)

9) Acceptable Use Policy & Enforcement

AspenView's terms prohibit:

- Illegal robocalls
- Fraudulent caller ID / spoofing violations
- Calls lacking required consumer consent (where applicable)
- Unlawful telemarketing activity

AspenView may pause, restrict, suspend, or terminate service for violations, and may require corrective action plans as a condition of continued service.

10) Recordkeeping & Program Updates

AspenView will maintain records supporting its robocall mitigation efforts and will update its RMD submission within **10 business days** of any material change to:

- Its traceback contact information,
 - Its mitigation measures,
 - Its STIR/SHAKEN implementation posture, or
 - Any other required certification elements.
-

Company Information (Replace-All Applied)

Company Name: AspenView Network Solutions

Phone: 1 866 312 8662

Address: 500 4th St NW, Suite 102, Albuquerque, NM 87102, United States

Designated Contact: Benjamin Pearson

Email: help@aspennetworks.com

Conclusion

AspenView Network Solutions submits this Robocall Mitigation Program in support of its RMD certification and affirms its commitment to mitigating illegal robocall traffic, cooperating with traceback efforts, and maintaining policies and controls aligned with applicable FCC rules.

