

Robocall Mitigation Program Description

Company Name: Advanced Network Communications LLC

Address: 1001 S. Main St. STE 600, Kalispell, Flathead County, MT 59901, USA

1. Overview

Advanced Network Communications LLC is a U.S.-based telecommunications provider offering VoIP services including wholesale voice termination, SIP trunking, DID services, and enterprise communication solutions.

We are committed to full compliance with the Federal Communications Commission (FCC) regulations related to robocall mitigation, unlawful traffic prevention, and caller authentication. Our robocall mitigation program is designed to detect, prevent, and eliminate illegal robocalls across our network.

2. STIR/SHAKEN Implementation

Advanced Network Communications LLC has fully implemented the STIR/SHAKEN framework:

- All IP-based outbound calls are signed using valid SPC tokens issued by an approved STI Certification Authority
 - Calls are attested at the appropriate level (A, B, or C) depending on customer relationship and verification level
 - Only authenticated and verified traffic is allowed to traverse our network
 - Calls failing authentication checks are flagged, restricted, or blocked
-

3. Customer Vetting & KYC Controls

We enforce strict onboarding procedures to prevent misuse of our network:

- Collection of company formation documents (EIN, Articles of Organization/Incorporation)
- Identity verification of company owners and authorized users
- Validation of business use case and traffic type (e.g., call center, enterprise, wholesale)

- Verification of contact details (email, phone, and business address)
- Screening against high-risk categories and fraud indicators

Only fully verified customers are permitted to originate traffic.

4. Traffic Monitoring & Fraud Detection

Advanced Network Communications LLC uses real-time monitoring systems and analytics tools to detect suspicious traffic patterns:

- Continuous monitoring of ACD (Average Call Duration), ASR (Answer-Seizure Ratio), CPS (Calls Per Second), and PDD
- Identification of short-duration, high-volume robocall patterns
- Detection of unusual call spikes, call bursts, or abnormal routing behavior
- Automated alerting system for fraud detection

Suspicious traffic is immediately flagged for investigation.

5. Call Blocking & Filtering Policies

We apply multiple layers of filtering to prevent illegal robocalls:

- Blocking of invalid, unallocated, or spoofed caller IDs
 - Enforcement of Do-Not-Call (DNC) compliance where applicable
 - Integration with industry reputation databases and blacklists
 - Filtering of high-risk destinations or traffic categories
 - Optional robocall filtering mechanisms such as analytics-based blocking
-

6. Traceback Cooperation & Response

We actively cooperate with traceback efforts coordinated by the U.S. Telecom Industry Traceback Group:

- Prompt response to traceback requests and regulatory inquiries
- Identification of originating customer and call path

- Immediate mitigation actions upon confirmation of suspicious activity
 - Sharing of relevant call data when legally required
-

7. Enforcement & Mitigation Actions

When suspicious or illegal robocall activity is detected:

- Immediate rate limiting or blocking of traffic
 - Temporary suspension of customer accounts pending investigation
 - Permanent termination of customers involved in violations
 - Reporting to upstream carriers or regulatory authorities if necessary
-

8. Network Security & Controls

- Strict access control for network infrastructure
 - Monitoring of SIP signaling and RTP media paths
 - Controlled routing policies to prevent unauthorized traffic flows
 - Media and signaling IP validation and filtering
 - Firewall and intrusion detection systems in place
-

9. Record Retention & Compliance

We maintain records to support compliance and investigations:

- Call Detail Records (CDRs) retention
 - STIR/SHAKEN authentication logs
 - Customer onboarding and KYC documentation
 - Incident and mitigation logs
-

10. Continuous Compliance & Improvement

Advanced Network Communications LLC continuously enhances its mitigation program:

- Regular updates based on FCC guidelines and industry best practices
 - Ongoing staff training on fraud detection and compliance
 - Deployment of improved analytics and fraud prevention tools
 - Periodic internal audits of network traffic and policies
-

11. Commitment Statement

Advanced Network Communications LLC enforces a strict zero-tolerance policy toward illegal robocalls. We are committed to maintaining a secure, compliant, and high-integrity telecommunications network and take immediate action against any misuse of our services.