



Robocall Mitigation Program (RMP)

Company Information

Business Name: American Telecommunications LLC

FRN: 0037163144

OCN: 602L

CEO: Tim Henning

EVP / Compliance Officer: Anuj Ghosal

Business Address: 1209 Mountain Road Pl NE, Ste N, Albuquerque, NM 87110, USA

Phone: +1 (877) 202-0074

Email: compliance@american-telecomm.com

Website: <https://www.american-telecomm.com>

1. Purpose and Scope of the Robocall Mitigation Program

American Telecommunications LLC ("American Telecommunications," "the Company," "we," or "our") has established this Robocall Mitigation Program (RMP) to comply with all applicable Federal Communications Commission (FCC) rules, orders, and guidance related to the prevention, detection, mitigation, and remediation of illegal robocalls, including but not limited to the rules adopted in FCC 20-42, FCC 21-123, FCC 22-37, and related enforcement advisories.

The purpose of this RMP is to:

- Prevent the origination, transit, or termination of illegal, unwanted, or fraudulent robocalls on our network.
- Ensure compliance with Section 64.6305 of the FCC's rules and all related robocall mitigation obligations.
- Protect consumers, enterprises, carriers, and public safety entities from unlawful robocalling activity.
- Maintain the integrity of the U.S. telecommunications ecosystem.
- Demonstrate ongoing, reasonable, and effective steps to mitigate the risk of illegal robocalls.

This program applies to **all traffic** that originates from, transits through, or terminates on American Telecommunications' network, including traffic



provided to or received from wholesale customers, retail customers, resellers, interconnected VoIP providers, SIP trunking customers, dialer platforms, and any other downstream or upstream carrier relationships.

2. Regulatory Framework and Compliance Commitment

American Telecommunications LLC is a U.S.-based telecommunications service provider operating under FCC authority and applicable federal and state regulations. The Company is committed to full compliance with:

- The Telephone Consumer Protection Act (TCPA)
- The Truth in Caller ID Act
- FCC robocall mitigation and call authentication rules
- STIR/SHAKEN implementation requirements
- The FCC Robocall Mitigation Database (RMD) filing and maintenance requirements

We recognize that illegal robocalls pose a serious threat to consumers and the telecommunications network. Accordingly, American Telecommunications maintains a zero-tolerance policy toward knowingly facilitating illegal robocalling, spoofing, fraud, scam traffic, or non-compliant dialing campaigns.

3. Network Overview and Traffic Profile

American Telecommunications LLC provides a range of telecommunications services, including but not limited to:

- Domestic U.S. VoIP termination
- Wholesale VoIP termination
- SIP trunking services
- Origination and termination services for enterprise and reseller customers
- SMS and messaging-related services (where applicable)



Traffic may include conversational voice calls, IVR calls, enterprise outbound campaigns, inbound customer service calls, and other lawful telecommunications use cases. Certain customers may utilize automated or dialer-based systems for lawful purposes such as appointment reminders, informational calls, or customer notifications.

All traffic is subject to strict onboarding, monitoring, and enforcement controls as described in this RMP.

4. STIR/SHAKEN Implementation

4.1 STIR/SHAKEN Status

American Telecommunications LLC has implemented STIR/SHAKEN call authentication technology across its IP-based network where technically feasible, in accordance with FCC mandates.

The Company:

- Signs outbound calls with appropriate attestation levels (A, B, or C) based on customer vetting and call origination knowledge.
- Verifies inbound calls using STIR/SHAKEN verification mechanisms.
- Works with upstream and downstream carriers to exchange authenticated traffic.

4.2 Attestation Management

- **Full Attestation (A):** Granted only to customers whose identity is fully verified and who are authorized to use the calling numbers.
- **Partial Attestation (B):** Applied where the customer identity is known but number authorization cannot be fully verified.
- **Gateway Attestation (C):** Used where traffic enters the network from an external source without full origination visibility.

Attestation levels are reviewed periodically and may be downgraded or revoked if compliance concerns arise.

5. Customer Due Diligence and Onboarding Procedures



American Telecommunications LLC applies comprehensive Know Your Customer (KYC) and Know Your Business (KYB) procedures before activating service for any customer.

5.1 Customer Verification

Prior to service activation, customers must provide, as applicable:

- Legal business name and registration documents
- EIN or tax identification number
- Proof of address
- Authorized contact details
- Description of intended traffic use cases
- Dialing methodology (manual, predictive, IVR, etc.)
- Sample calling scripts (where applicable)
- Confirmation of TCPA compliance and consent practices

5.2 High-Risk Traffic Assessment

Customers engaging in or proposing:

- High-volume outbound calling
- Automated or predictive dialing
- Lead generation or marketing campaigns
- Short-duration call patterns

are subject to enhanced due diligence, including additional documentation, testing, and monitoring prior to full production traffic approval.

6. Prohibited Traffic and Use Cases

American Telecommunications LLC strictly prohibits the use of its network for:

- Illegal robocalls
- Spoofed or misleading caller ID



- Scam, fraud, or phishing campaigns
- Calls violating TCPA or state consumer protection laws
- Calls to numbers on the National Do-Not-Call Registry without proper exemption or consent
- Snowshoeing, short-duration burst calling, or traffic obfuscation techniques

Any customer found to be engaging in prohibited activities is subject to immediate enforcement action.

7. Traffic Monitoring and Analytics

7.1 Continuous Monitoring

American Telecommunications employs real-time and post-call monitoring tools to analyze traffic patterns, including:

- Call volume and velocity
- Average Call Duration (ACD)
- Answer-Seizure Ratio (ASR)
- Post-dial delay and call completion metrics
- Repeated calling to invalid or unassigned numbers

7.2 Automated Alerts

Automated systems generate alerts for anomalous behavior, including:

- Sudden traffic spikes
- Extremely low ACD or ASR
- High complaint correlation
- Repeated short-duration calls

These alerts trigger immediate review by the Network Operations and Compliance teams.

8. Complaint Handling and Traceback Cooperation



8.1 Consumer and Carrier Complaints

American Telecommunications maintains internal procedures for receiving and investigating complaints from:

- Consumers
- Enterprise customers
- Upstream and downstream carriers
- Industry traceback organizations

All complaints are logged, investigated, and resolved in a timely manner.

8.2 Traceback Cooperation

The Company fully cooperates with:

- FCC enforcement inquiries
- Industry traceback requests
- Law enforcement agencies

Upon receipt of a traceback request, American Telecommunications promptly identifies the source of the traffic, preserves relevant records, and takes appropriate action, including suspension or termination where warranted.

9. Enforcement and Remediation Actions

When suspected illegal or non-compliant traffic is identified, American Telecommunications may take one or more of the following actions:

- Immediate traffic throttling or blocking
- Temporary suspension of the customer account
- Formal notice to the customer requesting explanation and remediation
- Permanent termination of service
- Reporting to upstream carriers or regulators where required

Enforcement actions are documented and retained as part of the Company's compliance records.

10. Recordkeeping and Documentation

American Telecommunications maintains records related to:

- Customer onboarding and verification
- Traffic monitoring and alerts
- Complaints and investigations
- Enforcement actions and resolutions
- STIR/SHAKEN attestation assignments

Records are retained in accordance with FCC requirements and internal compliance policies.

11. Employee Training and Compliance Governance

11.1 Training

Employees involved in network operations, customer onboarding, sales, and support receive periodic training on:

- Robocall mitigation requirements
- TCPA and FCC rules
- Identifying fraudulent traffic patterns
- Escalation and enforcement procedures

11.2 Compliance Oversight

The EVP / Compliance Officer, Anuj Ghosal, is responsible for overseeing this RMP, ensuring its effectiveness, and updating it as necessary to reflect regulatory changes or evolving risks.

12. Program Review and Updates

This Robocall Mitigation Program is reviewed at least annually and updated as needed to ensure continued compliance with FCC rules and industry best practices.



American Telecommunications LLC certifies that this RMP represents a good-faith, reasonable, and effective effort to prevent and mitigate illegal robocalls on its network.

13. Certification

American Telecommunications LLC hereby affirms that the information contained in this Robocall Mitigation Program is accurate and complete to the best of its knowledge and that the Company is actively implementing the measures described herein.

Authorized Signatory:

Tim Henning
Chief Executive Officer
American Telecommunications LLC

Date: 10/18/2025

