

Advanced Data & Network Solutions, Inc.

Robocall Mitigation Plan (Revised)

Business Address: 60 Ravenscroft Dr, Asheville, NC 28801

FRN: 0031494594

1. Company Overview and Compliance Status

Advanced Data & Network Solutions, Inc. (“ADNS”) is a voice service provider headquartered in Asheville, North Carolina. We provide hosted PBX services, SIP trunking, and direct SIP connectivity for business customers. We operate primarily as a non-facilities-based reseller of SIP trunking services. We do not directly interconnect to the public switched telephone network (PSTN). All outbound traffic from our customers is handed off to an upstream carrier for PSTN termination. Our upstream carrier (currently Bandwidth.com) is listed in the FCC’s Robocall Mitigation Database and implements the STIR/SHAKEN caller ID authentication framework. While we do not perform STIR/SHAKEN signing ourselves, calls originated by our customers are authenticated by our upstream carrier before entering the PSTN.

This Robocall Mitigation Plan describes the specific, reasonable steps we take to prevent the origination of illegal robocalls in compliance with 47 C.F.R. § 64.6305(a), and to ensure that our network is not used to facilitate unlawful traffic.

Prior FCC Action and Current Status

We have been the subject of formal regulatory action by the Federal Communications Commission (FCC) related to our Robocall Mitigation Database (RMD) certification.

On December 10, 2024, the FCC’s Enforcement Bureau issued a Show Cause Order (DA 24-1267), which was published in the Federal Register on December 17, 2024. That order directed us and other providers to cure deficiencies in our Robocall Mitigation Database certifications and robocall mitigation plans by applicable deadlines.

On August 6, 2025, the FCC issued an order removing our certification from the Robocall Mitigation Database due to deficiencies in our RMD certification, including insufficient detail and specificity regarding our robocall mitigation and Know Your Customer (KYC) practices as required by FCC rules.

On August 25, 2025, the FCC issued a subsequent order reaffirming the removal and including findings that our RMD certification remained deficient because it did not adequately describe required elements of our robocall mitigation program.

The enforcement action was initiated and conducted solely by the Federal Communications Commission. No other law enforcement or regulatory agencies were involved.

The FCC's findings were limited to deficiencies in our RMD certification and documentation. The FCC did not find that we transmitted unlawful robocalls, engaged in spoofing, or intentionally facilitated illegal robocall traffic.

The current status of this matter is remediation and compliance. We have submitted corrected information and this updated robocall mitigation plan addressing the FCC's findings. No final determination reinstating our RMD certification has yet been issued.

2. STIR/SHAKEN Implementation Status

We have a STIR/SHAKEN implementation obligation, but we do not implement STIR/SHAKEN on any portion of our own network at this time.

We do not maintain outbound PSTN gateways or SS7 interconnection facilities, we do not possess an STI certificate, and we do not operate an authentication service capable of signing calls. All outbound calls from our customers are routed exclusively to our upstream carrier (currently Bandwidth.com), which is certified in the FCC Robocall Mitigation Database and implements STIR/SHAKEN signing on the calls it sends to other carriers.

Because we lack the technical ability and network control to deploy STIR/SHAKEN directly, we rely on our upstream provider for call authentication and focus our efforts on a robust

robocall mitigation program. This plan describes the reasonable steps we take to prevent illegal robocalls from originating on our network, in lieu of local STIR/SHAKEN signing.

If our network architecture changes in the future, such as by deploying our own PSTN interconnects or gateways, we will obtain an STI certificate, implement STIR/SHAKEN signing as required, and update this plan accordingly.

3. Robocall Mitigation Practices

We have adopted a comprehensive Robocall Mitigation Program consisting of measures designed to detect, prevent, and respond to illegal robocall traffic on our network.

3.1 Traffic Monitoring and Analytics

We continuously monitor outbound call traffic for patterns indicative of illegal robocall activity, including high volumes of short-duration calls, sudden spikes in calls per minute or calls per second, sequential or neighbor spoofing calling patterns, repeated calls to the same destination in a short period, and call attempts using invalid or unallocated caller ID numbers.

To support this monitoring, we use internal analysis of call detail records as well as analytics provided by our upstream carrier, Bandwidth.com. These analytics include caller reputation scoring, detection of numbers on Do Not Originate lists, detection of invalid or unallocated numbers, and alerts for suspicious or high-risk traffic. Alerts generated by these analytics are promptly reviewed by our personnel. We do not currently use any additional third-party robocall analytics vendors beyond our upstream carrier.

3.2 Blocking of Suspected Illegal Traffic

Based on analytics and industry data, we block:

- Calls using numbers on known or industry-standard Do Not Originate lists;
- Calls using invalid, malformed, or clearly unassigned numbers as caller ID; and
- Traffic associated with known scam campaigns or identified illegal callers.

When we or our upstream provider identify specific numbers or ranges associated with unlawful robocalls, those numbers are added to blocking or screening lists to prevent further abuse.

3.3 Network Access Controls

To prevent unauthorized use of our network, we enforce strict access controls. All PBX extensions and user endpoints must authenticate via unique SIP credentials. SIP trunks and

direct SIP devices are restricted using IP allow-lists and other authentication controls. We may apply rate limits and concurrent call limits to specific customers or accounts to prevent abuse or sudden spikes in activity. These controls help ensure that only authorized, vetted customers can originate calls through our systems.

3.4 Enforcement Actions Against Customers

We maintain a formal enforcement process for customers whose traffic appears to involve illegal robocalls. When analytics, traceback, or complaints suggest that a customer may be originating illegal robocalls, we immediately investigate the traffic. If the investigation indicates potential violations or high-risk activity, we issue a written warning to the customer requiring immediate remediation and an explanation. We may impose stricter limits, require specific changes to calling practices, or temporarily suspend outbound service while an issue is investigated. If unlawful behavior is confirmed or the customer fails to remediate promptly, we terminate the customer's service and block further traffic from that source. This policy is reflected in our customer contracts and is consistently enforced.

4. Know-Your-Customer (KYC) Program

We maintain a robust Know-Your-Customer (KYC) program to prevent bad actors from obtaining service and to ensure that our customers are legitimate and compliant.

4.1 Onboarding and Identity Verification

Before enabling voice service for any new customer, we collect and verify:

- Legal name and business name;
- Form of organization;
- Tax identification number;
- Business address; and
- Contact information for a responsible officer or principal.

For individual or sole proprietor customers, we may obtain a government-issued ID. We verify this information using public records and other sources when appropriate.

4.2 Business Legitimacy and Use-Case Review

We evaluate the legitimacy of each customer's business and intended use of our service, including:

- Reviewing the customer's website or online presence;
- Confirming that the services requested are consistent with the customer's business; and
- Assessing whether the proposed calling patterns are typical and lawful for that type of customer.

Higher-risk use cases, such as high-volume outbound marketing, may trigger additional due diligence or restrictions.

4.3 Numbering Rights and Caller ID Validation

Where customers request to present specific telephone numbers as caller ID, we confirm that the customer has the legal right to use those numbers, for example by obtaining a Letter of Authorization or a copy of a relevant carrier invoice, or by assigning numbers directly to the customer through our upstream carrier. This helps prevent spoofing of numbers that do not belong to the customer.

4.4 Compliance and Sanctions Screening

We screen new and, where appropriate, renewing customers for indicators of past misbehavior, such as: • History of enforcement actions or litigation related to telemarketing, TCPA violations, or robocalling; and • Public reports linking the customer or its principals to illegal calling activity. Customers with problematic histories may be rejected, subject to additional conditions, or closely monitored.

4.5 Contractual Prohibitions

Our service agreements require that customers: • Comply with all applicable laws and regulations; • Refrain from originating illegal robocalls or spoofed traffic; • Cooperate fully with traceback requests and our investigations; and • Acknowledge that violations may result in immediate suspension or termination of service. Customers must accept these terms before service is activated.

4.6 Ongoing Review

KYC is not a one-time event. We periodically review customer accounts and traffic patterns for anomalies, may re-verify customer identity or business status upon renewal or significant change in service, and escalate unusual behavior for manual review and potential enforcement action.

5. Know-Your-Upstream-Provider Practices

Because we rely on upstream carriers to reach the PSTN, we also implement a Know-Your-Upstream-Provider program.

5.1 RMD and Compliance Verification

We only use upstream providers that are listed in the FCC Robocall Mitigation Database and that have certified either full or partial STIR/SHAKEN implementation and a robocall mitigation program. We verify the Robocall Mitigation Database status of our upstream partners and do not knowingly send or receive voice traffic from unlisted or non-compliant providers.

5.2 Contractual Requirements

Our contracts with upstream providers: • Prohibit the origination or transit of illegal robocall traffic; • Require the upstream provider to maintain its own STIR/SHAKEN implementation and robocall mitigation program; and • Require cooperation with traceback and enforcement requests.

5.3 Monitoring and Remediation

If we become aware that an upstream provider is associated with illegal robocall traffic affecting us or our customers, we will: 1. Notify the upstream provider and request immediate mitigation, such as blocking specific sources or traffic types; 2. Evaluate whether

calls from that provider continue to present a risk; and 3. If necessary, discontinue the relationship or re-route traffic to another compliant provider.

6. Traceback Cooperation and Response

We fully cooperate with traceback and enforcement efforts. We have designated a specific email address and contact person for robocall mitigation and traceback requests and commit to respond fully to all traceback requests within 24 hours of receipt. Upon receiving a traceback request, we identify the relevant calls in our records, determine the originating customer or upstream source, provide the requested information to the traceback initiator, and initiate an internal investigation and, where appropriate, enforcement actions against the responsible customer or partner. We document each traceback event and the steps taken in response.

7. Customer Education and Outreach

We provide information to customers about robocall risks and compliance obligations, including materials describing common robocall scams and illegal calling practices, guidance on lawful use of prerecorded or automated calls and the need for consent, direction to official consumer resources for robocall education, and periodic reminders and updates when significant regulatory changes or new scam patterns emerge. Customers are encouraged to report suspicious or abusive calling activity to us so we can investigate and take action.

8. Company Ownership and Contact Information

Legal Name: Advanced Data & Network Solutions, Inc. Business Address: 60 Ravenscroft Dr, Asheville, NC 28801 Country of Business Address: United States of America FRN: 0031494594 Foreign Voice Service Provider: No

Principals: • Jason Scheewe, Chief Executive Officer • Brian Scheewe, Chief Technology Officer

We have no parent company and no affiliates or subsidiaries that provide voice services.

Robocall Mitigation Contact: • Name: Brian Scheewe • Title: CTO • Department: Headquarters • Address: 60 Ravenscroft Dr, Asheville, NC 28801 • Telephone: 828-285-8882 • Email: brian@adnsolutions.com

This is our primary contact information for robocall mitigation and compliance matters.

9. Certification Statement

We certify that:

1. All calls we originate on our network are subject to the robocall mitigation program described in this document, consistent with 47 C.F.R. § 64.6305(a).

2. We do not implement STIR/SHAKEN on any portion of our own network at this time and rely on an upstream provider for STIR/SHAKEN signing.
3. We will update this plan if our network architecture or STIR/SHAKEN implementation status changes.
4. We will respond fully and in good faith to all traceback requests from the Commission, law enforcement, and the industry traceback consortium within 24 hours.
5. We will continue to refine and improve our robocall mitigation practices as industry standards and regulatory requirements evolve