

Business Automation Technologies Inc. dba Data Network Solutions

Caller ID Authentication Plan Updated February 20, 2026

I. Introduction.

Business Automation Technologies Inc. dba Data Network Solutions (“DNS”), FRN 0012077178, pursuant to Sections 64.6301 and 64.6305 of the Commission’s rules, 47 C.F.R. §§ [64.6301](#), [64.6305](#) and the Commission’s “Best Practices”¹ as amended² adopts this Caller ID Authentication (“Plan”). This Plan replaces all previous plans, is current as of its submission date, and may be subject to change as necessary to further comply with amended Commission regulations and requirements.

DNS has incorporated amendments to its Plan to further document DNS’s compliance with Commission Caller ID Authentication rules, including rules promulgated under the Commission’s *Eighth Report and Order* in its Advanced Methods to Target and Eliminate Unlawful Robocalls proceeding³ and *Eighth Report and Order* in its Call Authentication Trust Anchor proceeding.⁴

With this update, DNS incorporates amendments to its Plan to further document compliance with Commission Caller ID Authentication rules, most recently including rules promulgated under the *Report and Order* in its Improving the Effectiveness of the Robocall Mitigation Database and Amendment of Part 1 of the Commission’s Rules, Concerning Practice and Procedure, Amendment of CORES Registration System proceedings.⁵

This Plan is current as of its submission date and may be subject to change as necessary to further comply with amended Commission regulations and requirements.

¹ *Call Authentication Trust Anchor*, WT Docket No. 17-97 *Wireline Competition Bureau Invites Comment on Caller ID Authentication Best Practices*, WC Docket No. 20-324, *Wireline Competition Bureau Issues Caller ID Authentication Best Practices*, DA 20-1526 (December 22, 2020)

² *Advanced Methods to Target and Eliminate Unlawful Robocalls*, *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17- 97, *Sixth Report and Order*, *Fifth Report and Order*, *Order on Reconsideration*, Order, FCC 22-37 (May 20, 2022) and *Call Authentication Trust Anchor*, WC Docket No. 17-97, *Sixth Report and Order*, FCC 23-18 (March 17, 2023).

³ *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*; *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, *Eighth Report in Order*, FCC 25-15 (rel. February 28, 2025)

⁴ *In the Matter of Call Authentication Trust Anchor*, WC Docket No. 17-97, *Eighth Report and Order*, FCC 24-120 (rel. November 22, 2024).

⁵ *Report and Order*, WC Docket No. 24-213, MD Docket No. 10-234, [FCC 24-135](#) (January 8, 2025),

II. Company Information

The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues is as follows:

Isaac Fajerman
President
Business Automation Technologies Inc. dba Data Network Solutions
116 Oceanport Avenue
Little Silver, New Jersey 07739
Telephone: 732.756.0295
Email: IFAJERMAN@DNETIT.COM

Business Automation Technologies Inc. operates under the assumed name of Data Network Solutions.

II. Company Information, Continued

DNS is a privately-owned corporation. DNS individual owner and principal is Isaac Fajerman, President. DNS has no affiliates, has no subsidiaries, and is not owned by any other entity. The Company's principal exerts full control over DNS' operations.

DNS falls under a plain language definition of a Small Voice Service Provider serving less than 100,000 voice service subscriber lines, pursuant to Section 64.6304(a)(2) of the Commission's rules, [47 C.F.R. § 64.6304\(a\)\(2\)](#).⁶

DNS is not a foreign voice service provider, is not an intermediate or gateway provider, does not serve subscribers who are physically located outside of the U.S., and does not act as a wholesale provider originating calls on behalf of another provider or providers. DNS' OCN is 852B. DNS does not have direct access to telephone numbers from the North American Numbering Plan Administrator (NANPA) and/or the National Pooling Administrator.

III. Certification.

DNS certifies that it maintains a service provider code token and that its originating calls are authenticated through its third-party caller ID authentication provider, iConnectiv LLC, under an established service contract. DNS's third-party caller ID authenticator utilizes DNS's service provider token to authenticate all DNS subscriber originating calls. DNS has also deployed analytics applications that automatically analyze subscriber traffic for calling pattern anomalies that could be the result of robocalling, subject to further company investigation.

⁶ *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, *Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd 3260 (Mar. 31, 2020) (First Caller ID Authentication Report and Order and Further Notice), para. 40.

III. Certification, Continued

DNS certifies that it has not been prohibited from filing in the Robocall Mitigation Database. DNS certifies further that it has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing. And DNS certifies that at no time during the prior two years, has DNS been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

IV. Robocall Mitigation Plan

This Robocall Mitigation Plan addresses the steps DNS has implemented to eliminate unlawful calls originating on its network, in compliance with applicable Commission rules including:

- Know Your Customer - Subscriber Vetting
- Telephone Number Validation
- Contractual Prohibitions
- Caller ID Authentication
- Network Traffic Monitoring, Analysis, and Investigation
- Do-Not-Originate List
- Refusing Traffic from Unlisted Providers.
- Cooperation with the Commission, Industry Traceback Consortium, and Law Enforcement Agencies

Know Your Customer - Subscriber Vetting

DNS fully vets all subscribers before providing service to the subscriber. DNS obtains specific subscriber information including service locations and principals, if commercial subscribers, and verifies location for all subscribers. Further, DNS compares information provided by the subscriber against underlying carrier records to verify accuracy and authentication and validate subscriber information. Subscribers are served under a service agreement.

DNS monitors its subscribers' traffic for call, originating number and terminating number irregularities in conjunction with its underlying carriers, and should irregularities be determined, will immediately contact the subscriber as part of its investigatory process. DNS does not grant, nor can it grant, right-to-use telephone number resources.

Telephone Number Validation

For new subscribers, DNS will assign telephone numbers to the account, unless the account has ported from another subscriber. DNS will ensure that only those subscriber telephone numbers held by its subscribers may originate traffic. For toll-free numbers, DNS will verify the underlying ten-digit number and ensure that only calls from the assigned numbers may originate calls.

IV. Robocall Mitigation Plan, Continued

Contractual Prohibitions

Provisions in customer contracts, tariffs, and service guides prohibit any unlawful, abusive or illegal use of services. Contractual provisions also provide DNS the right to suspend or interrupt service that is being used to violate those policies. DNS will seek to identify the party that is using its network to originate such calls and take appropriate action under the customer's contract. DNS has updated its terms of service to expressly include a prohibition on the use of the service in any illegal, fraudulent, improper, inappropriate, and/or unauthorized manner.

Caller ID Authentication

Pursuant to Section 64.6301, Caller ID Authentication, 47 C.F.R. §§ 64.6301, DNS authenticates and verifies caller information for calls through its engagement of iconectiv LLC in conjunction with DNS's Service Provider Code (SPC).

Neustar authenticates calls generated by DNS subscribers using DNS's assigned SPC token under an established caller ID verification agreement. All domestic and international calls originating from DNS's network are authenticated, accordingly.

By incorporating this advanced certificate signing mechanism into its outbound call process, DNS mitigates the risk of fraudulent activities such as caller ID spoofing and establishes a reliable and secure framework for its subscribers. In so doing, DNS implements the STIR/SHAKEN caller ID authentication across its entire network and calls originated from its subscribers are compliant with 47 C.F.R. §§ 64.6301.

Network Traffic Monitoring, Analysis and Investigation.

Consistent with its commitment above, DNS will respond fully to all traceback requests from the Commission, law enforcement, and the industry traceback consortium as soon as possible and at no time exceeding 24 hours from the time of the request and will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

As necessary, DNS coordinates with its underlying carriers to monitor DNS' subscribers' traffic, to identify traffic anomalies including, but not limited to, unusually high call volumes to different telephone numbers and disparate geographic areas, over the course of one or more hours, for which DNS will investigate, and to immediately block subscriber service if robocalling is suspected. Confirmation of illegal activity and more than one violation will result in immediate service termination.

Do-Not-Originate List

Pursuant to the Commission's *Eighth Report and Order* in its Advanced Methods to Target and Eliminate Unlawful Robocalls proceeding, DNS is compiling a reasonable do-not-originate list. DNS's do-not-originate list excludes numbers that are deemed unreasonable for purposes of call origination in accordance with the criteria established pursuant to 47 C.F.R. § 64.1200, as they are discovered.

IV. Robocall Mitigation Plan, Continued

Refusing Traffic from Unlisted Providers.

In conjunction with its underlying carrier, DNS refuses to accept traffic from unlisted and de-listed providers from the Commission's Robocall Mitigation Database.

Cooperation with the Commission, Industry Traceback Consortium, and Law Enforcement Agencies

Pursuant to Section 64.6305 of the Commission's rules, 47 C.F.R. § [64.6305](#), DNS commits to take all such *reasonable steps* to avoid originating illegal robocall traffic and shall include a commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

DNS avers to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium within twenty-four (24) hours,⁷ and to cooperate with such entities in investigating and stopping any illegal robocallers that use DNS's service to originate calls.

If following internal investigation and investigation in conjunction with the industry traceback consortium, Commission, and/or law enforcement agencies, DNS confirms that any subscriber has engaged in – or allowed the engagement of – robocalling, DNS will immediately terminate its provision of service, and inform the Commission and Trust Anchor of the identity of the former subscriber and telephone numbers that were involved.

V. Commitment

DNS has implemented a call authentication protocol for voice calls delivered through its third-party vendor, iConnectiv, who performs call authentication on the Company's behalf.

DNS will ensure that it will update company information contained in the Commission Registration System (CORES) within ten business days from the date when information changes to reflect up-to-date Company information. Further, pursuant to Section 64.6305(h) of the Commission's rules, 47 C.F.R. § 64.6305(h) DNS affirmatively certifies and will recertify annually, that any information submitted to the Robocall Mitigation Database is true and correct on or before March 1.

DNS anticipates that its Plan will evolve as it makes Plan enhancements, as underlying carriers enhance their own plans, and as the Trust Anchor and industry generally gain experience in caller ID authentication protocols.

DNS avers to update its plan within ten business days from the date of any Plan changes.

[Signature on following page.]

⁷ Pursuant to 47 C.F.R. § 64.1200(n)(1) as clarified by the Commission.

February 20, 2026

Business Automation Technologies Inc., dba
Data Network Solutions

/s/ Isaac Fajerman

Isaac Fajerman
President
116 Oceanport Avenue
Little Silver, New Jersey 07739
Telephone: 732.756.0295