



Digital Network Access Communications Inc.

DECEMBER 2024



Address:

601 1st Ave Rochelle IL 61068

Phone Number

(815) 562-4290

Robocall Mitigation Plan

Pursuant to 47 C.F.R. § 64.6305, Digital Network Access Communications Inc. submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures. Digital Network Access Communications Inc. (hereinafter also referred to as "DNA Communications" or "The Company") has a temporary plan in place to mitigate illegal robocalls. The Company may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time to respond to changes in its business, its capabilities and its needs.

DNA Communications has enforceable terms of use and/or an acceptable use policy noted in its contracts. These policies define the circumstances by which the company will deny, suspend, or terminate service to a customer. The company has a vetting and review process for upstream providers, that is, providers that send us voice traffic that the company terminates or transits to other providers.

DNA Communications confirms that the upstream providers have a certification in the Robocall Mitigation Database. The company will not accept voice traffic from an unregistered provider. The Company has been informed of the upstream providers "Know-Your-Customer" guidelines and have provided them with the necessary KYC documentation they've requested that the company complete.

DNA Communications follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

This process includes the collection and review of entity-identifying information to confirm that the company has an authenticated relationship with the customer. The Company uses this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

DNA Communications also validates, when possible, that the entity has a legitimate right to use its asserted calling numbers. The Company uses this information to support the attestation level it assigns to calls that it originates for that customer.

DNA Communications contractual provisions with customers prohibit them from initiating illegal robocalls. If the Company discovers a customer is initiating suspicious robocalls, the company will temporarily suspend the service until the issue can be investigated. If it is discovered that the call was in fact fraudulent or a robocall, then the Company terminates their service.

DNA Communications requires that upstream providers have a reasonable Robocall Mitigation Plan, including a vetting process for their customers as well as their upstream providers, and that they use call analytics to identify suspicious traffic.

Prior to installing services for new customers, the company takes the following measures to weed out end users that could potentially generate robocall traffic:

The Company uses a KYCs to confirm the following information for its customers:

- **Customer's identity**
- **Customer's right to use the telephone number presented on calls**
- **Service Address**
- **Credit History**
- **Business Incorporation Documents**

DNA Communications will comply fully with all conditions set forth in the FCC'S 2024 Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.

DNA Communications has designated an individual as a dedicated point of contact for addressing traceback requests. It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>. The Company will respond promptly to inquiries from the Industry Traceback Group (ITG) within 24 hours.

If a pattern of questionable activity is detected, DNA Communications requires its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated. Requests from the ITG must be submitted in writing and include the following information:

Phone Number in Question:

Called Party Number

Date / Time Stamp

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

DNA Communications will provide valid law enforcement and regulatory agencies with the relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities, and implement mandated Robocall Mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls. The company will respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. The company will cooperate fully with such entities in investigating and stopping any illegal robocallers that use the Company's service to originate, carry, or process illegal robocalls.

Requests from the valid agency must be submitted in writing and include the following information:

Law Enforcement Agency Name:

Agency Address:

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

DNA Communications is not subject to any Commission, Law Enforcement, or Regulatory Agency Action or investigation due to suspected unlawful robocalling or spoofing. The company has not had any Robocall complaints.

DNA Communications does not wish to publicize any private and/or classified information that has the potential to expose the Company to fraud and/or anti-competitive actions. Therefore, the Company will submit a redacted version for the public site and requests that the FCC keep the unredacted version CONFIDENTIAL.