

EXHIBIT 1

We represent ALN Medical Management (“ALN”), located at 3401 Village Drive, Suite 200, Lincoln, NE 68516, and are writing to notify your Office of an incident that may affect the security of information relating to certain Massachusetts residents. ALN is providing notice on behalf of the client entities below:

- National Spine and Pain, 5280 Corporate Drive, Suite C-250, Frederick, MD 21703
- Inpatient Physician Associates, LLC, 3200 Pine Lake Road, Suite A Lincoln, NE 68516
- Hoag Clinic, 2995 Red Hill Avenue, Suite 100 Costa Mesa, CA 92626
- Allied Physicians Group, 175 Broad Hollow Road, Suite 150, Melville, NY 11747

Notice and the investigation in this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ALN does not waive any rights or defenses regarding the applicability of Massachusetts law, the applicability of the Massachusetts data event notification statute, or personal jurisdiction.

Nature of the Data Event

In March 2024, ALN identified suspicious activity related to certain systems being hosted by a third-party service provider. Upon learning of this activity, ALN promptly took steps to ensure the security of ALN systems, isolated the impacted environment, and launched an investigation to determine the nature and scope of the activity. While the incident did not impact internal ALN systems, the investigation determined that certain files and folders within the third-party hosted environment were accessed or taken by an unauthorized actor between March 18, 2024 and March 24, 2024. As a result, ALN began an extensive programmatic and manual review of these files and folders to determine whether sensitive information may be impacted, and to whom the information relates. Following this extensive review, ALN undertook an in-depth analysis of the results to identify the individuals associated with the information and to which ALN clients the information belonged. On or about January 31, 2025, ALN completed this process and provided notice of this incident to potentially impacted clients. ALN coordinated notifications with the potentially impacted clients and is providing notice to individuals and regulators, as directed, on its clients’ behalf.

Although the information varies for each individual, the potentially impacted data includes name, Social Security number, and financial account information.

Notice to Massachusetts Residents

On or about March 21, 2025, ALN provided written notice of this incident, which includes approximately 258 Massachusetts residents, notified relevant media outlets, and placed notice of this incident on its website. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. Notification to impacted individuals is ongoing and ALN may supplement this notification if it is determined that a significant number of additional Massachusetts residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, ALN moved quickly to investigate and respond to the incident, assess the security of ALN’s systems, and identify potentially affected individuals and ALN clients. Further, ALN notified law enforcement regarding the event and is also reviewing existing security policies and implemented additional measures to further protect against similar incidents moving forward. ALN is providing access to complimentary credit monitoring services for twenty-four (24) months, through IDX, to all potentially impacted individuals affected by this incident.

Additionally, ALN is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and explanation of benefits, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. ALN is providing notice of this incident to relevant state and federal regulators, including the U.S. Department of Health and Human Services, and the three credit reporting agencies.

Please be advised that, consistent with G.L. c. 93H § 3(b), ALN maintains policies and procedures that are substantially similar to a written information security program ("WISP").

EXHIBIT A



Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/ALN>

March 21, 2025

NOTICE OF <<Variable Text 2>>

Dear <<First Name>> <<Last Name>>:

ALN Medical Management (“ALN”) is writing to inform you of an incident that may impact the security of some of your information. ALN is a professional services firm that provides revenue cycle and billing services to its clients, including <<Variable Text 3>>. We are providing you with information about the incident, our response, and steps you may take to better protect against identity theft and fraud, should you feel it is necessary to do so.

What Happened? In March 2024, ALN identified suspicious activity related to certain systems being hosted by a third-party service provider. Upon learning of this activity, we promptly took steps to ensure the security of our systems, isolated the impacted environment, and launched an investigation to determine the nature and scope of the activity. The investigation determined that certain files and folders within our third-party hosted environment were accessed or taken by an unauthorized actor between March 18, 2024 and March 24, 2024. This incident did not impact internal ALN systems. As a result, ALN began an extensive review of these files and folders to determine whether sensitive information may be impacted.

What Information Was Involved? Our review determined that information related to certain individuals was present in the involved files and folder. Following this determination, we undertook an in-depth review process to identify the individuals and ALN clients who were potentially impacted and notified <<Variable Text 3>>. ALN is notifying you now out of an abundance of caution because the information involved in this incident includes your <<Variable Text 1>>, and name.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon becoming aware of this incident, we immediately took steps to confirm the security of our network. We reviewed existing security policies and implemented additional measures to further protect against similar incidents moving forward. We also reported this incident to law enforcement and regulators.

In addition to providing you with notice of the event, we are also offering you immediate access to complimentary credit monitoring and identity theft protection services for <<12/24>> months, through IDX. You can find information on how to enroll in these services in the below *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please scan the QR code above for enrollment, go to <https://response.idx.us/ALN>, or call our dedicated assistance line at 1-877-720-6166 Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time, excluding U.S. holidays. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

ALN Medical Management

Steps You Can Take To Help Protect Your Information

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/ALN> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is June 21, 2025.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-877-720-6166 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and <https://oag.dc.gov/>. ALN is located at 3401 Village Drive, Suite 200, Lincoln NE 68516.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. ALN is located at 3401 Village Drive, Suite 200, Lincoln NE 68516.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 245 Rhode Island residents that may be impacted by this event.