WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

January 30, 2026

Joseph M. Fusz
312.821.6141 (Direct)
joseph.fusz@wilsonelser.com

Via Online Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Cybersecurity Incident Involving Alpine Ear, Nose, & Throat, P.C.

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Alpine Ear, Nose, & Throat, P.C. ("AENT"), a healthcare provider that provides specialized medical care located at 1120 East Elizabeth Street, Suite F-101, Fort Collins, CO 80524, with respect to a cybersecurity incident that was first discovered by AENT on November 19, 2024 (hereinafter, the "Incident"). AENT takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maine residents being notified, and the steps that AENT has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On November 19, 2024, AENT discovered that its systems were potentially compromised by an unauthorized actor. Upon discovery of this Incident, AENT promptly worked with their Managed Services Provider (MSP) to secure their systems and engaged a specialized third- party cybersecurity firm to conduct a forensic investigation of its network environment to determine the nature and scope of the Incident. The forensic investigation concluded that personal information within AENT's systems was subject to unauthorized access. While the investigation was ongoing, on January 17, 2025, AENT posted substitute notice on its organization's website.

Based on these findings, AENT began a comprehensive and thorough review of the impacted information, including data mining, to identify the specific individuals and the types of data that were potentially accessed. On October 9, 2025, the data mining process was completed. Thereafter,

AENT worked to verify the individuals impacted and updated addresses for mailing individual notice letters. On January 26, 2026, AENT finalized the list of individuals to notify.

Although Alpine ENT is unaware of any fraudulent misuse of information, it is possible that Demographic Information, Date of Birth, Medical Information, Health Insurance Information, and for some individuals, Financial Account Information, Credit Card CVC, Credit Card Expiration, Credit Card Number, Social Security Number may have been exposed as a result of this unauthorized activity.

As of this writing, AENT has not received any reports of related identity theft since the date of the incident (November 19, 2024, to present).

2. Number of Maine residents affected.

AENT identified 65,648 individuals potentially affected by this Incident. Of those, ten (10) were residents of Maine. Notification letters to these individuals were mailed on January 30, 2026, by US First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

AENT is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, AENT moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, AENT engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident and has taken additional steps to reduce the risk of this type of incident occurring in the future by enhancing technical security measures and procedures. Lastly, AENT informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although AENT is not aware of any actual or attempted misuse of the affected personal information, AENT offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through IDX to all individuals to help protect their identity. Additionally, AENT provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact information

AENT remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please contact me at joseph.fusz@wilsonelser.com or 312-821-6141.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Joseph M. Fusz

EXHIBIT A

ALPINE
EAR, NOSE & THROAT, P.L.L.C.
P.O. Box 989728
West Sacramento, CA 95798-9728

Via First-Class Mail

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

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: April 30, 2026
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

January 30, 2026

Re: Notice of Data Security <<Variable Text: Header>>

Dear <<First Name>> <<Last Name>>,

Alpine Ear, Nose, & Throat, P.C. ("AENT") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to some individuals' personal information. While we are unaware of any fraudulent misuse of personal information at this time, this notice is intended to provide details about the incident, steps we are taking in response, and resources available to help protect against the potential misuse of personal information.

What Happened?

On November 19, 2024, AENT discovered that its systems were potentially compromised by an unauthorized actor. Upon discovery of this incident, AENT promptly worked with their Managed Services Provider (MSP) to secure their systems, and engaged a specialized third- party cybersecurity firm to conduct a forensic investigation of its network environment to determine the nature and scope of the Incident. The forensic investigation concluded that certain personal information within AENT's systems was subject to unauthorized access.

Based on these findings, AENT began a comprehensive and thorough review of the impacted information, including data mining, to identify the specific individuals and the types of data that were potentially accessed. On October 9, 2025, the data mining process was completed. Thereafter, AENT worked to verify the individuals impacted and updated addresses for mailing individual notice letters. On January 26, 2026, AENT finalized the list of individuals to notify.

What Information was Involved?

Although AENT has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. The information impacted varied by individual. Based on the investigation, Alpine ENT determined that the following information related to you may have been subject to unauthorized access: <<Variable Text: Data Elements>> and Name.

What We Are Doing:

Data privacy and security is among our highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, we have taken additional steps to reduce the risk of this type of incident occurring in the future by enhancing our technical security measures and procedures.

We are also providing you with access to **Single Bureau Credit Monitoring** services at no charge. These services provide you with alerts for <<12/24>> months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided through IDX.

What You Can Do.

We encourage you to take advantage of the complimentary credit monitoring and identify theft protection we are making available to you. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below. Additionally, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. You can find more information on steps to protect yourself against identity theft identity theft in the enclosed *Additional Resources to Help Protect Your Information* sheet.

How do I enroll for the free services?

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is April 30, 2026.

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 1-844-427-0772 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information.

If you have any questions or concerns not addressed in this letter, please call 1-844-427-0772 (toll free) Monday through Friday, during the hours of 8 a.m. and 8 p.m. Central Standard Time (excluding U.S. national holidays).

AENT sincerely regrets any concern or inconvenience this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Alpine Ear, Nose, & Throat, P.C.

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information on how to file such a complaint by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx. <<Variable Text: MD State>>

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.