



May 23, 2024

Brian H. Myers, Esq. (CIPP/US)
(202) 626-7695
Brian.Myers@WilsonElser.com

Via Email:

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Notice of Cybersecurity Incident

Office of the Attorney General:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Affiliated Dermatologists & Dermatologic Surgeons P.A. (“AD”), located at 182 South Street, Suite 1, Morristown, New Jersey, 07960, and is providing notice of a recent cybersecurity incident.

This letter will serve to inform you of the nature of the incident, what information may have been affected, the number of Maryland residents being notified, and the steps that AD has taken in response. We have also included a sample of the notification letter that AD mailed to the potentially impacted individuals on May 23, 2024, which includes an offer of free credit monitoring and identity theft protection services. By providing this notice, AD does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

1. Nature of the Incident

On March 5, 2024, AD detected it was the target of a cybersecurity attack whereby an unauthorized third party gained access and left a ransom note on AD’s network. Upon discovery of this incident, AD immediately disconnected access to the network, alerted its third-party IT provider, and engaged legal counsel and specialized cybersecurity professionals to conduct a forensic investigation.

On April 10, 2024, AD’s investigation determined that between March 2, 2024 and March 5, 2024, the unauthorized actor obtained access to certain systems and copied data from AD’s network, including the personal information of some AD patients and employees. AD then began analyzing the relevant data to confirm the identities of those individuals whose personal information was potentially involved for the purpose of notifying those individuals. While AD found that certain data was copied, AD’s investigation has not found any evidence indicating that any personal information has been misused for identity theft or fraud in connection with this incident.

On May 3, 2024, AD issued a public notice of the incident on the homepage of its website and issued a press release for distribution to major media. On May 23, 2024, AD mailed personalized notification letters to all affected individuals detailing the categories of information involved for

each individual and instructions for how to enroll in the credit monitoring and identity theft protection services that AD is providing free of charge.

2. Information and Number of Maryland Residents Affected.

A total of 507 Maryland residents may have been potentially affected by this incident. AD mailed personalized notification letters to these individuals on May 23, 2024.

While the information involved varies for each individual, AD's investigation has determined that the unauthorized actor may have accessed the following categories of information:

- For certain patients: name, date of birth, mailing address, social security number, medical treatment information, and health insurance claims information.
- For certain employees: name, date of birth, mailing address, social security number, driver's license number, and passport number.

Again, the information involved varies for each individual, and not every category applies in each individual case. On May 23, 2024, AD mailed personalized notification letters to the affected individuals that detail the specific categories of information that apply in each individual's case.

3. Steps taken in response to the Incident.

AD is committed to the security of personal information and is taking steps to prevent a similar incident from occurring. Upon discovery of the incident, AD moved quickly to investigate, respond, and confirm the security of its systems. Specifically, AD immediately disconnected access to its network and engaged legal counsel and specialized cybersecurity professionals to assist network restoration efforts and conduct a forensic investigation. In addition, AD enhanced its network security by implementing 24-7 network security monitoring, requiring multi-factor authentication for all remote access, and resetting passwords for all accounts on the network.

Although AD's investigation has not found evidence of any actual or attempted misuse of the affected personal information, AD offered complimentary credit monitoring and identity theft protection services to all affected individuals.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at Brian.Myers@WilsonElser.com or (202) 626-7695.

Regards,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in blue ink, appearing to read 'Brian H. Myers', is written over a light blue rectangular background.

Brian H. Myers, Esq.

Certified Information Privacy Professional – United States

Affiliated Dermatologists
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



May 23, 2024

Via First-Class Mail

Re: Notice of Data Security Incident

Dear [REDACTED]:

Affiliated Dermatologists (AD) is writing to inform you of a recent data security incident. We take the privacy and security of personal information in our care seriously. This notice will provide you with information about the incident, the steps we are taking in response, and actions you can take to help protect against the potential misuse of your personal information, including how to enroll in the free credit monitoring and identity theft protection services that we are offering.

What Happened:

On March 5, 2024, AD detected it was the target of a cybersecurity attack whereby an unauthorized third party gained access and left a ransom note on AD's network. Upon discovery of this incident, AD immediately disconnected access to the network, alerted its third-party IT provider, and engaged legal counsel and specialized cybersecurity professionals to conduct a forensic investigation into the nature and scope of the incident.

On April 10, 2024, AD's investigation determined that between March 2, 2024 and March 5, 2024, the unauthorized actor obtained access to certain systems and copied data from AD's network, including the personal information of AD patients and employees.

What Information Was Involved:

AD's investigation determined that the copied data may have included the following categories of your personal information: [REDACTED]

At this time, AD is not aware of any personal information being misused for identity theft or fraud in connection with this incident.

What We Are Doing:

AD takes the privacy and security of personal information in our care seriously. Since the discovery of the incident, AD moved quickly to investigate, respond, and confirm the security of our systems. Specifically, AD immediately disconnected access to its network and engaged specialized cybersecurity professionals to assist network restoration efforts and conduct a forensic investigation into the nature and scope of the incident.

000010103G0500

P

In addition, AD has taken steps to further enhance its network security, including implementation of 24-7 network security monitoring, multi-factor authentication for all remote access, and password resets for all accounts on the network.

As part of our ongoing commitment to the security of your personal information, we are offering you access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) 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 by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Please see the following section for instructions on how to enroll in those services.

What You Can Do:

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. Please review the enclosed *Additional Information about Identity Theft Protection* to learn more about how to protect against the possibility of identity theft.

We also encourage you to enroll in the credit monitoring and identity theft protection services that we are offering at no cost. Please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided to enroll. When prompted please provide the following unique code to receive services: [REDACTED]. Please note that the code is case-sensitive and will need to be entered as it appears.

You must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled you will have twelve (12) months of monitoring services. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information:

We take this incident and the security of personal information in our care seriously. If you have additional questions, representatives are available for 90 days from the date of this notice to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, at the following toll-free number: **1-833-549-9899**.

Sincerely,

Robert Lombardi
Chief Executive Officer
Affiliated Dermatologists

Additional Information About Identity Theft Protection

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.



FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached 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. Instances of known or suspected identity theft should also be reported to law enforcement.

This notice was not delayed as a result of any law enforcement investigation.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, you have the right to obtain a 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 Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act at 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, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

For Oregon residents, you are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).



