WILSON ELSER

November 3, 2021

Mary Park
213.330.8747 (direct)
Mary.Park@wilsonelser.com

Via Certified Mail; Return Receipt Requested

Attorney General John Formella
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Notice of Data Breach

Re:	**Our Client**	**:**	**Baywood Medical Associates, PLC dba Desert Pain Institute ("DPI")**
	Matter	**:**	**Data Security Incident on September 13, 2021**
	Wilson Elser File #	**:**	**16516.01631**

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Baywood Medical Associates, PLC dba Desert Pain Institute ("DPI"), a health care provider specializing in pain management, located in 6309 E Baywood Ave., Mesa, AZ 85206, with respect to a data security incident that was first discovered by DPI on September 13, 2021 (hereinafter, the "Incident"). DPI 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 New Hampshire residents being notified, and the steps that DPI 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 September 13, 2021, DPI detected and stopped a network security incident. Upon discovery of this incident, DPI promptly secured and began remediating our network. DPI also engaged a specialized third-party cybersecurity firm to conduct a comprehensive investigation to determine the nature and scope of the incident. On October 15, 2021, the forensic investigation concluded DPI's system was compromised between July 3, 2021 to September 13, 2021, and found evidence that some DPI files were available to the unauthorized actor during the incident.

Although DPI is unaware of any fraudulent misuse of information, it is possible that individuals' full name, address, date of birth, Social Security number, tax identification number, driver's license/state-issued identification card number, military identification number, financial account number, medical information, and health insurance policy number may have been exposed as a result of this unauthorized activity. Not all of these data elements were compromised for each individual.

As of this writing, DPI has not received any reports of related identity theft since the date of the incident (September 13, 2021 to present).

2. Number of New Hampshire residents affected.

DPI identified and notified one (1) resident of New Hampshire. Notification letter to this individual was mailed on November 3, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken in response to the Incident.

DPI 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, DPI moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, DPI engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, DPI enhanced the security measures for its systems and servers, and installed end-point monitoring tools to continuously monitor its system. Lastly, DPI informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although DPI is not aware of any actual or attempted misuse of the affected personal information, DPI offered 12 months of complimentary credit monitoring and identity theft restoration services through IDX to all individuals to help protect their identity. Additionally, DPI 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

DPI remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Mary.Park@wilsonelser.com or 213-330-8747.

WILSON ELSER

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Mary Park, Esq.

Enclosure: *Sample Notification Letter*

Desert Pain Institute
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-608-3032
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

November 3, 2021

Re: Notice of data breach

Dear <<FirstName>> <<LastName>>,

Baywood Medical Associates, PLC dba Desert Pain Institute ("DPI") is writing to inform you of a recent data security incident that may have exposed your sensitive personal information. At this time, we are unaware of any misuse of your personal information. However, we take the security of your personal information seriously and wanted to provide you with details about the event, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened and What Information was Involved?

On September 13, 2021, DPI detected and stopped a network security incident. Upon discovery of this incident, DPI promptly secured and began remediating our network. DPI also engaged a specialized third-party cybersecurity firm to conduct a comprehensive investigation to determine the nature and scope of the incident. On October 15, 2021, the forensic investigation concluded and found evidence that some DPI files were available to the unauthorized actor during the incident.

This letter serves to notify you that it is possible the following information related to you, if provided to DPI, may have been exposed to the unauthorized party: full name, address, date of birth, Social Security number, tax identification number, driver's license/state-issued identification card number, military identification number, financial account number, medical information, and health insurance policy number. We maintained this information for patient care and administrative purposes. Notably, the types of information affected varied by individual, and not every individual had every element exposed.

As of this writing, DPI has not received any reports of related identity theft since the date of the incident (September 13, 2021 to present).

What We Are Doing

We are committed to doing everything we can to help protect the privacy and security of the personal information in our care. Since the discovery of the incident, we have taken and will continue to take steps to mitigate the risk of future issues. Notably, upon discovery of the incident, we moved quickly to initiate our incident response plan, which included conducting an investigation with the assistance of the third-party forensic specialists to contain and safely restore our systems. We are also enhancing our security measures for our systems and servers, and have installed end-point monitoring tools to continuously monitor our system.

Out of an abundance of caution, we are also providing you with <<12/24>> months of complimentary credit monitoring services through IDX. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

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. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the credit monitoring services we are making available to you.

We are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-608-3032 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above.

Again, we are making these services available to you at no cost; however, you will need to activate yourself in these services. The deadline to enroll is February 3, 2022.

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

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-833-608-3032 (toll free) during the hours of 6 a.m. and 6 p.m. General Mountain Time, Monday through Friday (excluding U.S. national holidays).

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

Sincerely,

Eric J. Boyd, M.D., partner/owner
Richard J. Ruskin, M.D., partner/owner
Baywood Medical Associates, PLC dba Desert Pain Institute

Steps You Can Take to Help Protect Your Information

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. As of September 21, 2018, 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	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	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. As of September 21, 2018, 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	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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 in order 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.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your 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 residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You 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 residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island*: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov