

May 16, 2022

Ross M. Molina, Esq.
504.702.1726 (direct)
Ross.Molina@WilsonElser.com

Via electronic-mail: Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re:	Our Client	:	Heidell Pittoni Murphy & Bach LLP
	Matter	:	Data Security Incident on December 25, 2021
	Wilson Elser File #	:	16516.01733

Dear Attorney General Frosh:

We represent Heidell Pittoni Murphy & Bach LLP (“HPMB”) with respect to a data security incident described in more detail below. HPMB takes the security and privacy of the information in its control 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 security breach, the number of Maryland residents that were potentially affected, what information has been compromised, and the steps that HPMB is taking to secure the integrity of its systems. We have also enclosed hereto samples of the notifications made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On December 25, 2021, HPMB was the target of a cybersecurity incident. An unauthorized third party attempted to infiltrate HPMB’s computer systems. Following the incident, HPMB’s forensic experts conducted an extensive investigation, which concluded on April 22, 2022. Based on the investigation, HPMB determined that certain information, including names, dates of birth, social security numbers, and certain medical treatment information, was part of a tranche of data accessed and briefly held by the unauthorized party.

HPMB, however, is not aware of any evidence that information has been further misused. HPMB has not received any reports of related identity theft since the date of the incident (December 25, 2021 to present).

2. Maryland Residents Notified

A total of 67 residents of Maryland were potentially affected by this security incident. Notification letters to these individuals will be mailed on May 16, 2022, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon learning of this incident, HPMB moved quickly to institute a response plan, which included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to confirm the security of any relevant systems. The FBI was also notified. HPMB has reviewed, altered and enhanced its policies and procedures relating to the security of its systems and servers, as well as its information life cycle management.

Although HPMB is not aware of any evidence of misuse of personal information, HPMB extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

4. Contact Information

HPMB 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 Ross.Molina@WilsonElser.com or 504.702.1726.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Ross M. Molina

Copy: Robert Walker, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letters*



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

To Enroll, Please Call:
(833) 940-2336
Or Visit:
<https://response.idx.us/hpmb>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

Via First-Class Mail

May 16, 2022

Notice of Data Incident

Dear <<Full Name>>:

Heidell Pittoni Murphy & Bach LLP (“HPMB”) serves as litigation counsel for New York Presbyterian Hospital in medical malpractice cases. In this role, HPMB receives medical records for some of New York Presbyterian Hospital’s patients. We recently discovered that a data security incident resulted in the unintentional exposure of some of your personal information. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself. Please be assured that HPMB takes the protection and proper use of your personal information very seriously, and we sincerely apologize for any inconvenience this may cause.

What Happened

On December 25, 2021, HPMB detected suspicious activity within its network environment. Upon discovery, we worked with our information technology (IT) support team and immediately engaged a law firm specializing in cybersecurity and data privacy to investigate further. Additionally, HPMB engaged third-party forensic specialists to assist HPMB in its analysis of any unauthorized activity. The preliminary assessment showed that an unauthorized person or entity gained control over certain of the firm’s information for a period of time until HPMB was able to negotiate its return.

Following the incident, HPMB’s experts conducted an extensive investigation, which concluded on April 22, 2022. Based on the investigation, we have determined that certain of your information, including your name, date of birth, social security number, and certain medical treatment information, was part of a tranche of data accessed and briefly held by the unauthorized party.

At this time, HPMB does not have any evidence to indicate that, since its return to us, any of your personal information has been or will be further misused as a result of this incident.

What We Are Doing

Upon detecting this suspicious activity, we moved quickly to initiate a response, which included conducting an investigation with the assistance of third-party forensic specialists and confirming the security of our network environment. We have ensured that no further unauthorized activity has continued. We have also reviewed and updated our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management. We will also be reporting this incident to the appropriate authorities.

HEIDELL, PITTONI, MURPHY & BACH, LLP

NEW YORK | CONNECTICUT | WESTCHESTER | LONG ISLAND

We value the safety of your personal information and are, therefore, offering credit monitoring and identity theft protection services through IDX. IDX's services include: <<12/24>> months of credit monitoring and fully managed id theft recovery services. With this protection, IDX will notify you and assist you to resolve issues if your identity is compromised.

What You Can Do:

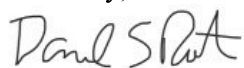
We encourage you to enroll in free IDX services by going to <https://response.idx.us/hpmb> and using the Enrollment Code provided above. Please note the deadline to enroll is August 16, 2022.

Enclosed hereto you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information

We recognize that you may have questions not addressed in this letter. We encourage you to contact IDX with any questions and to enroll in free IDX services by calling (833) 940-2336, Monday through Friday, 9 am to 9 pm Eastern Time.

Sincerely,

A handwritten signature in dark ink, appearing to read "Daniel S. Ratner". The signature is fluid and cursive, with the first name "Daniel" and last name "Ratner" clearly distinguishable.

Daniel S. Ratner

Additional 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.

Security Freeze: You also 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:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/ personal/credit-report-services/ credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/ center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/ credit-freeze
---	--	---

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, 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 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.

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

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.