



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

August 30, 2024

Bruce A. Radke
312-819-1900
bradke@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of Data Security Incident

Dear Mr. Karberg:

We represent Hospital Sisters Health System (“HSHS”), 4936 LaVerna Road, Springfield, Illinois 62579, in connection with an incident that involved the personal information of twelve (12) Maryland residents. HSHS is reporting the incident pursuant to Md. Code Ann, Com. Law § 14-3504(h). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While HSHS is notifying you of this incident, HSHS does not waive any rights or defenses relating to the incident, this notice, or the applicability of Maryland law on personal jurisdiction.

NATURE OF THE INCIDENT

On August 27, 2023, Hospital Sisters Health System (HSHS) discovered an unauthorized third party gained temporary access to HSHS’s network. Upon learning of the situation, HSHS immediately took steps to contain and remediate the incident and launched an internal investigation. HSHS also reported the incident to law enforcement and engaged a leading forensic security firm to assist in the investigation and confirm the security of the HSHS computer systems and network. The forensic investigation determined that the unauthorized third party accessed certain files on the HSHS network between August 16 and August 27, 2023. HSHS has since been reviewing those files and notifying individuals whose information was found in the files on a rolling basis as their review has continued.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California

98062785.1

August 30, 2024

Page 2

NOTIFICATION TO MARYLAND RESIDENTS

HSHS is notifying the twelve (12) residents of Maryland whose personal information was contained in the files involved in the incident. These notifications are being made via letters mailed by USPS First Class Mail on August 30, 2024. The notification letters describe the incident and provide information on ways the individuals can protect themselves against potential fraud and identity theft and include an offer of complimentary credit monitoring and identity theft protection services. HSHS has also arranged for a toll-free, dedicated call line to assist the notified individuals with any questions they may have regarding the incident. Enclosed is a sample of the letter.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, HSHS began an internal investigation. As mentioned, HSHS is notifying employees and patients whose information was contained in the files and is offering complimentary credit monitoring and identity theft protection services.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,



Bruce A. Radke

Enclosure



Hospital Sisters

HEALTH SYSTEM

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Dear <<Name1>>:

Hospital Sisters Health System (HSBS) cares deeply about our colleagues, and that is why we are writing to update you regarding an incident that may have involved some of your personal information. This letter tells you what happened, what information was potentially accessed, what HSBS is doing in response to the incident, and provides guidance on what you can do to protect yourself, should you feel it is important to do so.

What Happened? As you may be aware, on August 27, 2023, HSBS discovered an unauthorized third party gained temporary access to HSBS's network. Upon learning of the situation, we immediately took steps to contain and remediate the incident and launched an internal investigation. We also reported the incident to law enforcement and engaged a leading forensic security firm to assist in our investigation and confirm the security of our computer systems and network. The forensic investigation determined that the unauthorized third party accessed certain files on our network between August 16 and August 27, 2023. We have since been reviewing those files and notifying individuals whose information was found in the files on a rolling basis as our review has continued.

What Information Was Involved? The type of information varied for each individual, but may have included your name, address, date of birth, and Social Security number and/or driver's license number. At this time, we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident from occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offering a free one-year membership of Experian IdentityWorksSM Credit 3B. This service helps detect possible misuse of your personal information and provides you with identity protection services including immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. Again, while we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring offer included in this letter. You can learn about more steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

For More Information. We value the trust you place in us to protect the privacy and security of your information and deeply regret any inconvenience or concern this incident might cause. For further information and assistance, please call [REDACTED] from 8:00 am - 8:00 pm Central, Monday through Friday, except major U.S. holidays.

Sincerely,

A handwritten signature in cursive script that reads "Melanie Wade".

Melanie Wade
System Privacy Officer

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Activation Code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-7378. Be prepared to provide engagement number <<Engagement #>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 833-931-7378 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 833-931-7378.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: By law, you have the right to place a fraud alert on your credit report if you believe you have been, or are about to become, a victim of fraud or related crime. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com/protectYourIdentity.action.

Credit and Security Freezes: By law, you have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
<https://www.equifax.com/persona/credit-report-services/credit-freeze/>
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
<https://www.experian.com/freeze/center.html>
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
<https://www.transunion.com/credit-freeze>
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney General to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's Office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's Office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New Mexico: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.