



900 W. 48th Place, Suite 900, Kansas City, MO 64112 • 816.753.1000

June 2, 2023

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

The Honorable John M. Formella
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Data Security Incident

Dear Attorney General Formella:

We represent the Howard County Library System (“HCLS”), 9411 Frederick Road | Ellicott City, MD 21042, in connection with an incident that may have involved the personal information of one New Hampshire resident. HCLS is reporting the incident pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While HCLS is notifying you of this incident, HCLS does not waive any rights or defenses relating to the incident or this notice.

NATURE OF THE INCIDENT

On February 21, 2023, HCLS discovered that an unknown, unauthorized third party accessed one (1) HCLS employee’s email account. Upon identifying the incident, HCLS promptly secured the email account and began an internal investigation. HCLS also engaged a forensic security firm to assist with its investigation. The forensic investigation determined that the third party accessed the email account at times between February 17, 2023, and February 21, 2023.

HCLS is not aware of any fraud or identity theft to any individual as a result of this incident and is not aware of evidence that the third party actually viewed or acquired any particular personal information contained in the email account. Nevertheless, because there was unauthorized access to the email account, HCLS reviewed the account’s contents to identify any personal information that had a possibility of being viewed by the third party.

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



June 2, 2023

Page 2

On April 19, 2023, HCLS completed its review and identified personal information pertaining to one New Hampshire resident. The personal information potentially involved in the incident included

NUMBER OF RESIDENTS NOTIFIED

HCLS will be notifying the one potentially involved New Hampshire resident of the incident via letter on June 2, 2023. The notification letter includes information on ways the individual can protect themselves against potential fraud and identity theft, as well as a telephone number they can call if they have any questions regarding the incident. The notification letter includes an offer for complimentary credit monitoring and identity theft protection through Experian. Enclosed is a copy of the notice that is being sent to the individual via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon discovering the incident, HCLS promptly secured the email account, began an internal investigation, and engaged a forensic security firm to further investigate and confirm the security of its email and computer systems. As mentioned, HCLS notified the individuals whose personal information may have been involved in the incident. HCLS also provided complimentary credit monitoring to individuals depending on the sensitive personal information involved. HCLS has taken steps to reduce the risk of this type of incident occurring in the future, including enhancing its technical security measures.

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,

Alexander D. Boyd

Enclosure



[REDACTED]

June 2, 2023

RE: NOTICE OF DATA BREACH

Dear [REDACTED]

We are reaching out to notify you that Howard County Library System (“HCLS”) recently learned that we were the possible subject of a breach involving the personal information of certain employees and other related individuals. We highly respect and take seriously our responsibility to the privacy of your personal information, which is why we are writing to advise you of this incident.

While we have no evidence that your personal information has been misused, we want to provide you with guidance and resources should you decide it appropriate to take additional precautions to ensure your information is protected.

What Happened? We recently learned that an unknown, unauthorized third party gained access to an HCLS employee’s email account. Upon discovering the incident, we promptly secured the email account and began an internal investigation. We also engaged a forensic security firm to investigate and confirm the security of our email and computer systems. This investigation determined that the third party accessed the email account between February 17, 2023, and February 21, 2023.

What Information Was Involved? In reviewing the contents of the compromised email account, it was determined that it contained personal employee information as well as that of certain dependents and relatives. This personal information included your [REDACTED]. While our review determined that this personal information was contained in the email account, our investigation did not find evidence confirming that the third party viewed any of this information.

What We Are Doing. In addition to the actions described above, HCLS has taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft involving your personal information, 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 identity protection services focused on prompt 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 additional information on identity theft prevention and IdentityWorks Credit 3B offer, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

What You Can Do. While we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can

also find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call _____ from 9 a.m. – 5 p.m. Eastern, Monday through Friday.

Sincerely,

Howard County Library System
9411 Frederick Road
Ellicott City, MD 21042

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: (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll:
3. PROVIDE the **Activation Code:** [REDACTED]
4. PROVIDE the necessary information when prompted

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 877-288-8057. Be prepared to provide engagement number [REDACTED] 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 ExtendCARE™:** 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 877-288-8057 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 877-288-8057.

* 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: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies 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 one of 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: You may want to consider placing a fraud alert on your credit report. 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.

Credit and Security Freezes: You may 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 can be placed without any charge and 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 www.equifax.com P.O. Box 105788 Atlanta, GA 30348 | Experian Security Freeze 1-888-397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013 | TransUnion Security Freeze 1-888-909-8872 www.transunion.com P.O. Box 160 Woodlyn, PA 19094 |
|---|--|---|

This notification was not delayed by law enforcement.

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 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.