

Colin M. Battersby
Direct Dial: (248) 593-2952
E-mail: cbattersby@mcdonaldhopkins.com

November 27, 2024

VIA EMAIL (Idtheft@oaq.state.md.us)

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

Re: Van Buren Public Schools – Incident Notification

To whom it may concern:

McDonald Hopkins PLC represents Van Buren Public Schools (“VBPS”). I am writing to provide notification of an incident on behalf of VBPS that may affect the security of personal information of two Maryland residents. By providing this notice, VBPS does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or around December 4, 2023, VBPS experienced a network security incident that impacted some operations. Upon detecting the incident, VBPS commenced an immediate and thorough investigation. As part of the investigation, VBPS worked to identify what personal information, if any, might have been compromised.

After a thorough investigation into the incident and extensive manual document review, VBPS discovered on October 28, 2024, that between approximately November 29, 2023 and December 4, 2023, a limited amount of information stored on VBPS’s network may have been accessed and/or acquired by an unauthorized party. This information included full names and or more of the following data points: Social Security number, health benefits and enrollment information, medical history, condition, treatment, and or diagnosis.

VBPS is not aware of any reports of identity fraud as a direct result of this incident. However, out of an abundance of caution, VBPS wanted to inform your Office (and the affected residents) of the incident. Affected residents will be notified of the incident starting on November 27, 2024, in substantially the same form as the letter attached hereto. The notified residents will be provided with best practices to protect their information, including but not limited to complimentary credit monitoring services to the extent their Social Security number was impacted. VBPS will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. VBPS will advise the affected

residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, and the Federal Trade Commission.

At VBPS, protecting the privacy of personal information is a top priority. VBPS is committed to maintaining the privacy of personal information in its possession and has taken precautions to safeguard it. VBPS continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com.

Very truly yours,



Colin M. Battersby

Encl.



Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Van Buren Public Schools ("VBPS"). We are writing with important information regarding a cyber-security incident that involved some of your information. We want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or around December 4, 2023, VBPS experienced a network security incident that impacted some operations.

What We Are Doing.

Upon learning of this issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on October 28, 2024, that between approximately November 29, 2023 and December 4, 2023, a limited amount of information stored on our network may have been accessed and/or acquired by an unauthorized individual.

What Information Was Involved?

The impacted information contained your name and the following: [REDACTED]

What You Can Do.

We have no evidence that your information has been misused for identity theft or financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are providing you with access to 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 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 provided in this letter.



This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 am - 7:00 pm Eastern Time.

Sincerely,
Van Buren Public Schools

[REDACTED]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you [REDACTED] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [REDACTED]
- Provide your **activation code**: [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by [REDACTED]. 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 MEMBERSHIP**

A credit card is not required for enrollment in Experian IdentityWorks. 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.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one (1) year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

* * * * *

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.