



A business advisory and advocacy law firm®

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

June 15, 2023

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

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

Re: Des Moines Public Schools - Security Breach Notification

Dear Mr. Brown:

We are writing on behalf of our client, Des Moines Public Schools (“DMPS”) (located at 2100 Fleur Drive, Des Moines, IA 50321) to notify you of a data security incident involving eight (8) Maryland residents. By providing this notice, DMPS does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Nature

On or about January 9, 2023, DMPS discovered suspicious activity in certain computer systems and subsequently learned this was a result of a ransomware incident. At that time, DMPS’ technology team acted quickly to evaluate and secure its systems. DMPS also engaged third-party independent cybersecurity experts to conduct an investigation into the incident.

The investigation is ongoing, however, DMPS determined that this incident resulted in the exposure of some data that it maintains. At that time, DMPS began a comprehensive review of the impacted data to identify the individuals whose personal information was included. DMPS recently completed its review.

On May 8, 2023, DMPS concluded its review and, on June 5, 2023, DMPS located the most recent contact information for these individuals. DMPS determined that the incident potentially involved eight (8) Maryland residents.

The personal information obtained potentially included first and last name in addition to one or more of the following data elements: address, phone number, email address, date of birth, bank account and routing number, Social Security number, driver’s license, state or student identification number, passport

number, medical information, and health insurance information. Not all data elements were impacted for all potentially affected individuals.

Notice and DMPS' Response to the Event

On June 16, 2023 DMPS will mail a written notification to the potentially affected Maryland residents, pursuant to Md. Code Ann., Com. Law § 14-3501-3508, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, DMPS is providing the potentially impacted individuals the following:

- Free access to credit monitoring services for one year through TransUnion;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, DMPS provided notice to the applicable government regulators, officials, and other state Attorneys General (as necessary). Finally, DMPS is working to implement any necessary additional safeguards; enhance and improve its policies and procedures related to data protection; improve its cybersecurity infrastructure; and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 456-2741 or email me at spollock@mcdonaldhopkins.com.

Sincerely Yours,

A handwritten signature in blue ink, appearing to read 'Spencer S. Pollock'.

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

[Redacted]

[Redacted]

[Redacted]



June 16, 2023

Re: Notice of a Data Security Incident

Dear [Redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Des Moines Public Schools (“DMPS”). We’re writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, what we did in response, and steps you can take to protect yourself against possible misuse of the information.

What Happened?

On January 9, 2023, DMPS became aware of suspicious activity in certain computer systems. When we discovered this, our technology team acted quickly to stop the activity and investigate the nature and scope of the activity with the assistance of third-party forensic specialists. Our investigation into the incident is ongoing, however, we recently determined that this incident resulted in the exposure of some data that we maintain.

On May 8, 2023, after completing an extensive review, we discovered that certain personal information was contained within the data impacted by this incident. ***However, at this time, there is no evidence of financial fraud or identity theft related to this data.***

What Information Was Involved.

The information impacted by this incident included [Redacted]

What We Are Doing.

Following this incident, DMPS took immediate steps to improve the security of the data we maintain. We are working to add further technical safeguards to our systems in addition to robust existing security measures. In an abundance of caution, we are also offering impacted individuals access to complimentary credit monitoring services.

What You Can Do.

We encourage individuals to review the “Other Important Information” below, which provides details on steps individuals can take to help protect personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. If your bank account information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

000010103G0500

P

[REDACTED]

Finally, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information.

We apologize for any concern this causes you, and we sincerely appreciate your patience as we continue our efforts to resolve this matter. 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 additional questions, please contact the external, dedicated call center we set up at [REDACTED] between the hours of [REDACTED], excluding holidays.

Sincerely,

Matthew A. Smith
Interim Superintendent
Des Moines Public Schools
2100 Fleur Drive
Des Moines, IA 50321

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

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



2. 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.

3. 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.

4. 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.

00001020380000

P

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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 2001, <https://oag.dc.gov/consumer-protection>, Telephone: 1-202-727-3400.

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; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

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.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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.

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

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting 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.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

Rhode Island Residents: Under Rhode Island law, individuals have the right to obtain any policy report filed in regard to this event. You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, (401) 274-4400.



There was approximately 1 Rhode Island resident that may be impacted by this incident.

00001030300000

P