McDonald Hopkins
A business advisory and advocacy law firm®

100 International Drive
23rd Floor
Baltimore, MD 21202

P 1.248.646.5070
F 1.248.646.5075

May 11, 2023

VIA EMAIL (DOJ-CPB@doj.nh.gov)
Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Rochester Public Schools - Security Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Rochester Public Schools ("Rochester") (615 7th St. SW, Rochester, MN 55902-2052) to notify you of a data security incident involving one (1) New Hampshire resident.[1]

Nature

On April 6, 2023, RPS detected unauthorized activity on its systems. RPS immediately engaged our firm and third-party cybersecurity experts to conduct a thorough investigation of the incident's nature and scope and to assist in the remediation efforts. Such remediation efforts include the implementation of endpoint detection and response software, password resets, and a review and audit of all accounts and software applications for up-to-date operating systems and security patches. The remediation efforts are ongoing.

The investigation is in its early stages; therefore, RPS has not yet determined the method of compromise nor the full scope of the incident. RPS recently determined that an unauthorized individual accessed RPS's systems and, as a result, obtained some data, including information belonging to current and former employees. On April 17, 2023, RPS determined that the incident affected the personal information of one New Hampshire resident. Further, on or about May 2, 2023, RPS located the most recent contact information for this individual.

The personal information obtained potentially included

. We have no evidence that the affected data has been used for financial fraud or identity theft.

[1] By providing this notice, RPS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Notice

On May 4, 2023, RPS mailed a written notification to the affected New Hampshire resident, pursuant to N.H. Rev. Stat. § 359-C:19 *et seq*., in a substantially similar form as the enclosed letter (attached as Exhibit A.)

In addition, RPS is providing the impacted individual 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, RPS provided notice to the applicable government regulators, officials, and other state Attorneys General (as necessary).

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 .

Sincerely Yours,

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

EXHIBIT A

Rochester Public Schools
[redacted]

[redacted]

May 4, 2023

Re: Notice of a Data Security Incident

Dear [redacted]:

The privacy and security of the data we maintain is of the utmost importance to Rochester Public Schools. We are writing with important information regarding a data security incident that involved some of your information. We want to inform you about the incident, explain the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On April 6, 2023, we detected unauthorized activity on our systems. We launched an investigation into the incident with the assistance of independent third-party cybersecurity experts. During our initial investigation, we determined that an unauthorized individual accessed our systems and, as a result, obtained some data, including information belonging to current and former employees. Our review is ongoing, but we recently determined that the data contained some of your personal information. Therefore, we wanted to notify you of the incident and provide you with steps you can take to help protect your information. **Please note, at this time, we have no evidence that the affected data has been used for financial fraud or identity theft.**

What Information Was Involved?

The affected data contained

.

What We Are Doing

The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to further secure our systems and engaged third-party forensic experts to assist in the investigation.

What You Can Do

We are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in 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]. This code should not be shared with anyone.

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.

Additionally, if you are interested in learning about how you can contact the Federal Trade Commission and obtain information from credit reporting agencies about fraud alerts and security freezes, you may refer to the "Other Important Information" included with this letter.

For More Information

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. If you have any additional questions, representatives are available for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday. Please call [redacted] and supply the fraud specialist with your unique code listed above.

Sincerely,

Kent Pekel
Superintendent of Schools
Rochester Public Schools
615 7th St SW, Rochester, MN 55902

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 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 access the request form at https://www.annualcreditreport.com/index.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax	***Experian***	***TransUnion***
P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below).

Equifax Security Freeze	***Experian Security Freeze***	***TransUnion Security Freeze***
P.O. Box 105788 Atlanta, GA 30348-5788 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (888)-298-0045	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze (888) 909-8872

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*,

Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/.

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.

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: 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; https://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.