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

March 15, 2024

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Newton Public Schools - Incident Notification

Dear Mr. Formella:

We are writing on behalf of our client, Newton Public Schools ("Newton") (located at 308 East First, Newton, KS 67114-3846) to notify you of a data security incident involving two (2) New Hampshire residents. By providing this notice, Newton does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On or around March 28, 2023, Newton Public Schools detected suspicious activity on its network involving a potential ransomware incident. Upon identifying the activity, Newton acted quickly to contain the threat, investigate, and ensure the security of its systems with the assistance of third-party forensic specialists. The investigation revealed that an unauthorized actor gained access to Newton' systems on or about March 23, 2023, and as a result likely obtained some information. On February 19, 2024, after an extensive forensic investigation and review, Newton discovered that certain personal information was included within the files that were subject to unauthorized access or acquisition as a result of the incident. Further, on February 23, 2024, Newton located the most recent contact information for these individuals and identified two (2) New Hampshire residents whose information was involved.

The personal information contained within the impacted data included

. The types of impacted information varied by individual. Newton has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, Newton wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected

residents against identity fraud. Newton is providing the affected residents with notification of this incident, commencing on or about March 15, 2024. The notice will be in substantially the same form as the letter attached hereto. Newton is also offering the affected residents whose Social Security number was potentially impacted by the incident with complimentary membership with a credit monitoring service. Newton is advising the affected residents to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. Newton is also advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected residents are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

[redacted]

Newton Unified School District 373

[redacted]

[redacted]

NEWTON PUBLIC SCHOOLS

March 15, 2024

IMPORTANT INFORMATION - PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing with important information regarding a recent cyber security incident at Newton Public Schools that may involve your personal information. We wanted to provide you with information about the incident, inform you about 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 or about March 28, 2023, we experienced unauthorized access to our network.

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. We concluded our extensive forensic investigation and manual document review on February 19, 2024 and determined that on or about March 23, 2023 an unauthorized actor gained access to our network and likely obtained certain files containing your personal information.

What Information Was Involved.

The impacted files contained your .

What You Can Do.

We have no evidence that any of your information has been misused. Nonetheless, out of an abundance of caution, to help protect your identity, we are offering a complimentary membership in Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services from Cyberscout through Identity Force, a TransUnion company at no charge. For more information on identity theft prevention and the Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services, including instructions on how to activate your complimentary 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.

P 0000101G03G0500

[redacted]

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 [redacted], Monday through Friday, 8:00 am to 8:00 pm EST, excluding holidays.

Sincerely,

Newton Public Schools
McKinley Administrative Center
308 East First
Newton, KS 67114-3846

[redacted]

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary Credit Monitoring.

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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 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
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 LLC
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
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.

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.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; 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.

[redacted]

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.