MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 28, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent City of Nashua School District ("NSD") located at 229 Main St., PO Box 2019, Nashua, NH 03061, and are writing to notify your office of an incident that may affect the security of certain personal information relating to eight thousand one hundred seventeen (8,117) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, NSD 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.

Nature of the Data Event

On April 28, 2023, NSD discovered unusual activity occurring within certain parts of its computer network. NSD quickly began working with third-party computer specialists to understand the nature and scope of the activity. NSD's investigation determined that it was the victim of a sophisticated cybersecurity attack involving ransomware, and that certain NSD systems were accessed by an unknown actor between March 30, 2023, and April 28, 2023. NSD worked with subject matter specialists to rebuild its environment in a safe and secure manner and initiated an exhaustive review of its systems to confirm the files that may have been accessed without authorization. NSD then worked with a specialized team to conduct a comprehensive review of the impacted files to determine if they contained personal information, and, if so, to whom the information related. NSD recently completed this assessment and is notifying potentially impacted individuals out of an abundance of caution.

The information that could have been subject to unauthorized access includes .

Notice to New Hampshire Residents

On or about February 28, 2024, NSD provided written notice of this incident to eight thousand one hundred seventeen (8,117) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, NSD moved quickly to investigate and respond to the incident, assess the security of NSD systems, and identify potentially affected individuals. Further, NSD notified federal law enforcement regarding the event. NSD is also working to implement additional safeguards and training to its employees.

Additionally, NSD is providing impacted individuals with guidance on how to better protect against identity theft and fraud. NSD is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, 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, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

NSD is providing written notice of this incident to relevant regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at

Very truly yours,

Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/dtg
Enclosure

EXHIBIT A

Secure Processing Center
20 Oser Ave, Suite 100
Hauppauge, NY 11788

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

NOTICE OF <<SECURITY INCIDENT>> / <<DATA BREACH>>

Dear <<First Name>> <<Last Name>>:

City of Nashua School District ("NSD") is writing to notify you about a recent incident that may involve some of your personal information. This notice provides you with information about the incident, our response, and additional steps you may take to protect your information, should you determine it is appropriate to do so.

What Happened? On April 28, 2023, we discovered unusual activity occurring within certain parts of our computer network. We quickly began working with third-party computer specialists to understand the nature and scope of the activity. Our investigation determined that we were the victim of a sophisticated cybersecurity attack involving ransomware, and that certain NSD systems were accessed by an unknown actor between March 30, 2023, and April 28, 2023. We worked with subject matter specialists to rebuild our environment in a safe and secure manner and initiated an exhaustive review of our systems to confirm the files that may have been accessed without authorization. We then worked with a specialized team to conduct a comprehensive review of the impacted files to determine if they contained personal information, and, if so, to whom the information related. We received the results of this assessment and are notifying potentially impacted individuals out of an abundance of caution.

What Information Was Involved? While we have no evidence that any personal information has been misused, we are notifying you about the potential exposure of your information out of an abundance of caution. The personal information that was stored on the affected NSD systems included your name, <<breached elements>>.

What We Are Doing. Upon discovering this incident, we quickly took steps to investigate and respond, including reviewing and enhancing our existing policies, procedures, and system security to reduce the likelihood of a similar future event. We also reported this incident to federal law enforcement and are notifying individuals and relevant state authorities, as required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity. You may also review and consider the information and resources outlined in the below "Steps You Can Take to Help Protect Personal Information."

For More Information. If you have additional questions, please call our dedicated assistance line at 888-321-4177 (toll free), Monday through Friday, from 9 am - 9 pm Eastern Time (excluding U.S. holidays). You may write to NSD at 229 Main St., PO Box 2019, Nashua, NH 03061 with any additional questions you may have.

Sincerely,

City of Nashua School District

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.