LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Kevin W. Yoegel
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Kevin.Yoegel@lewisbrisbois.com
Direct: 215.253.4255

April 1, 2022

VIA ELECTRONIC MAIL
Attorney General John Formella
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General John Formella:

We represent the Altoona Area School District ("AASD") with respect to a recent data security incident described in greater detail below.

1. Nature of the security incident.

On or about December 2, 2021, AASD detected unusual activity impacting certain systems. Upon discovering this activity, AASD took steps to secure its network and launched an investigation, with the assistance of a leading digital forensics firm, to determine what happened and whether personal information had been accessed or acquired without authorization. Through this investigation, AASD AASD learned that certain AASD systems potentially containing personal information had been accessed without authorization as part of the incident. AASD then worked diligently to identify up-to-date address information required to notify potentially-impacted individuals. On March 14, 2022, AASD confirmed that the personal information of three (3) New Hampshire residents was contained on an impacted system and therefore may have been accessed or acquired without authorization. Specifically, the personal information involved may included three (3) resident's name, date of birth and Social Security number.

2. Number of New Hampshire resident(s) affected.

AASD notified three (3) residents of New Hampshire of this data security incident via first class U.S. mail on April 1, 2022. A sample copy of the notification letter sent to the potentially-affected individuals is included with this correspondence.

3. Steps taken relating to the incident.

In response to the incident, AASD retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the incident. AASD also reported this matter to law enforcement and will provide whatever assistance is necessary to hold the perpetrator(s) of this incident accountable. Additionally, AASD has taken steps to enhance its digital security to help prevent a similar incident from occurring in the future. Finally, AASD is notifying potentially-affected individuals and providing them with steps they can take to protect their personal information, including by enrolling in the complimentary identity monitoring services being offered.

4. Contact information.

AASD remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (215) 253-4255 or by e-mail at Kevin.Yoegel@lewisbrisbois.com.

Respectfully,

/s/ Kevin W. Yoegel

Kevin W. Yoegel of
LEWIS BRISBOIS BISGAARD & SMITH LLP

KWY:SGG

Encl.: Sample Consumer Notification Letter
cc: Shaun G. Goodfriend, Associate, Lewis Brisbois Bisgaard & Smith LLP

P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-648-2053
Or Visit:
https://response.idx.us/AASD
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

April 1, 2022

Re: Notice of Data Security Incident

Dear <<FIRST NAME>> <<LAST NAME>> <<Suffix>>,

We are writing to inform you of a data security incident that may have involved some of your personal information. At Altoona Area School District ("AASD"), we are committed to the security of all information within our possession. This is why we are writing to notify you of this incident, to offer you complimentary identity monitoring services, and to inform you about steps that can be taken to help safeguard your personal information.

What Happened. On December 2, 2021, we detected unusual network activity impacting certain systems. Upon discovering this, we immediately initiated an investigation and took steps to secure our network. We also engaged third-party digital forensics experts to assist with the investigation and determine whether sensitive information may have been accessed or acquired during the incident. Through our investigation, which was completed in March of 2022, we learned that certain files containing some of your personal information were accessed or acquired without authorization during the incident. We then took steps to identify up-to-date address information and notify you.

What Information Was Involved. The incident impacted information included your first name, last name, in combination with <<Variable Text 1>>.

What Are We Doing. As soon as we discovered the incident, we took the steps described above. We also implemented enhanced security measures to help prevent a similar incident from occurring in the future. We also notified the Federal Bureau of Investigation and will fully cooperate with any investigation. In addition, out of an abundance of caution, AASD is offering you complimentary identity protection services through IDX, a data security and recovery services expert. This complimentary two-year enrollment in IDX identity protection includes: credit and CyberScan monitoring, a $1 million insurance reimbursement policy, and fully managed identity theft recovery services. Additional information about these services is included with this letter.

What You Can Do. Please follow the recommendations included with this letter to help protect your personal information. You can also enroll in the IDX identity protection services being provided to you, at no cost, through IDX. To enroll, please visit the IDX website at https://response.idx.us/AASD and provide your enrollment code located at the top of this page. Please note that the deadline to enroll is July 1, 2022. Additional information describing the IDX identity protection services, along with other recommendations to protect your personal information, is included with this letter.

For More Information. Please accept our sincere apologies for any worry or inconvenience this incident might cause you. If you have any questions, please call us directly at 1-833-648-2053 from 9 a.m. to 9 p.m. Eastern Time.

Sincerely,

Dr. Charles Prijatelj
Superintendent of Schools
Altoona Area School District

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Two-Year Enrollment in IDX Identity Protection

Website and Enrollment. Please visit **https://response.idx.us/AASD** and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the credit monitoring provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at **1-833-648-2053** to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This IDX enrollment will include two-year enrollment into:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDX Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.