



Baker & Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

David B. Sherman
direct dial: 215.564.8380
dshe@bakerlaw.com

January 10, 2024

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

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

Re: Incident Notification

Dear Attorney General Brown:

We are writing on behalf of our client, National Association of Educational Procurement ("NAEP"), to notify you of a cybersecurity incident involving two Maryland residents.

NAEP recently concluded an investigation into an incident that involved unauthorized access to certain employee email accounts. Upon identifying the incident, NAEP took measures to secure the email accounts, began an investigation, and notified law enforcement. Through the investigation, NAEP determined that an unauthorized actor accessed these accounts between September 14, 2023, and October 14, 2023. NAEP was unable to rule out the possibility that emails and attachments in the email accounts may have been accessed during this incident. Accordingly, NAEP conducted a review of the emails and attachments in the mailboxes and, on November 20, 2023, identified emails or attachments containing the names and Social Security numbers of two Maryland residents.

On January 10, 2024, NAEP is mailing notification letters to the Maryland residents via United States Postal Service first-class mail. A sample copy of the notification letter is enclosed. NAEP is offering one year of complimentary identity monitoring services through IDX to the Maryland residents whose data was involved.

To help reduce the risk of a similar incident from occurring in the future, NAEP implemented additional security measures to enhance the security of its email system and is continuing to train its employees concerning data security.

January 10, 2024

Page 2

Please do not hesitate to contact me if you have any questions regarding this incident.

Sincerely,

A handwritten signature in black ink, appearing to read "David B. Sherman". The signature is fluid and cursive, with the first name "David" being more prominent.

David B. Sherman

Partner

Enclosure

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

January 10, 2024

Dear <<First Name>>:

National Association of Educational Procurement recognizes the importance of protecting the information we maintain. We are writing to inform you that we identified and addressed a data security incident that may have involved your information. This letter explains the incident, the measures we have taken, and steps you may consider taking in response.

We completed an investigation of an incident involving unauthorized access to certain employee email accounts. Upon discovering the incident, we took measures to secure the email accounts and began an investigation. We also contacted law enforcement. Through our investigation, we determined that an unauthorized actor accessed these accounts between September 14, 2023 and October 14, 2023. We were unable to rule out the possibility that emails and attachments in the email accounts may have been accessed during this incident. Accordingly, we conducted a review of the mailboxes and, on November 20, 2023, determined that an email or attachment contained your name and Social Security number.

We encourage you to remain vigilant by reviewing your credit reports for any unauthorized activity. As a precaution, we are offering identity theft protection services through IDX, A ZeroFox Company. IDX identity protection services include: [12 months/24 months] of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. **For instructions on how to activate your complimentary [one/two]-year membership and steps you may consider taking in response to this incident, please see the pages that follow this letter.**

To help prevent another incident from occurring, we have implemented additional security measures to enhance the security of our email system and we are continuing to train our employees concerning data security. If you have any questions about the incident, please call me at (443) 543-5527, Monday through Friday, between 8:00 a.m. and 5:00 p.m., Central Time.

Sincerely,



Byron Burr Millsap
Director of Accounting & Finance
National Association of Educational Procurement



IDX Identity Protection Services

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using the following Enrollment Code: **XXXXXX**. Please note the deadline to enroll is November 1, 2024.

2. Activate the credit monitoring provided as part of your IDX identity protection 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.

3. Telephone. Contact IDX at **1-800-939-4170** to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

National Association of Educational Procurement's phone number is 443-543-5527 and its mailing address is PO Box 18188, Oklahoma City, OK 7315.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov/

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

Rhode Island: This incident involves 1 individual in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov