McDonald Hopkins
A business advisory and advocacy law firm®

**David Lane**

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

March 18, 2025

**VIA Email**

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

**Re: Pennsylvania State Education Association – Incident Notification**

Dear Attorney General Formella:

McDonald Hopkins PLC represents Pennsylvania State Education Association ("PSEA"). I am writing to provide notification of an incident at PSEA that may affect the security of personal information of approximately 67 New Hampshire residents. By providing this notice, PSEA does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

PSEA experienced a data security incident on or about July 6, 2024. Upon learning of this issue, PSEA immediately commenced a prompt and thorough investigation. As part of the investigation, PSEA engaged external cybersecurity professionals who regularly investigate and analyze these types of situations to help determine the extent of any compromise of the information on the PSEA network. It was determined that an unauthorized actor accessed or acquired certain files from the PSEA network. We discovered on February 18, 2025, that certain files containing personal information in the possession of PSEA were impacted by the incident. The impacted data includes

. Not all data elements were impacted for every individual.

To date, PSEA is not aware of any incidents of identity fraud or financial fraud as a result of the incident. Nevertheless, out of an abundance of caution, PSEA is providing notice to impacted individuals. The notifications are provided via substitute notice, under New Hampshire - N.H. Rev. Stat. §§ 359-C:19-21 (d), including publication to state media and notice on the PSEA website together with email notice to those individuals for whom PSEA has email addresses. This notice commenced on or around March 17, 2025, in substantially the same form as the enclosed (Attached as Exhibit A). The notified individuals who have had their impacted will receive complimentary credit monitoring services. Additionally, PSEA has advised all affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. PSEA has further advised the

affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents have also been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority for PSEA. PSEA remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. PSEA continually evaluates and modifies practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at . Thank you for your cooperation.

Very truly yours,

David Lane

Encl.

# Exhibit A

PENNSYLVANIA STATE EDUCATION ASSOCIATION

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

[redacted]

Enrollment Code: [redacted]

To Enroll, Scan the QR Code Below:

[redacted]

SCAN ME

Or Visit:

[redacted]

[redacted]

***IMPORTANT INFORMATION***
***PLEASE REVIEW CAREFULLY***

Dear [redacted]:

I am writing with important information regarding a recent data security incident at the Pennsylvania State Education Association ("PSEA"). The privacy and security of the protected personal information entrusted to us is of the utmost importance to PSEA. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

*What Happened?*

We experienced a security incident on or about July 6, 2024 that impacted our network environment. Through a thorough investigation and extensive review of impacted data, which was completed on February 18, 2025, we determined that the data acquired by the unauthorized actor contained some personal information belonging to individuals whose information was contained within certain files within our network. We took steps, to the best of our ability and knowledge, to ensure that the data taken by the unauthorized actor was deleted. We want to make you aware of the incident and provide you with steps you can take to further protect your information.

*What We Are Doing.*

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked closely with external cybersecurity professionals and notified law enforcement of the incident. Additionally, PSEA is reviewing its existing policies and training protocols relating to data protection while enhancing security measures and monitoring tools to further mitigate risks of this nature.

*What Information Was Involved?*

The data taken by the unauthorized actor contained your [redacted]

*What You Can Do.*

**We have no evidence that any of your information has been used for identity theft or to commit financial fraud.** Nevertheless, out of an abundance of caution, we want to make you aware of the incident. We are also providing you with complimentary access to identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. The enrollment deadline is

We encourage you to enroll in the free identity protection services by calling [redacted], going to [redacted] or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

This letter also suggests other precautionary measures that you may 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.

*For More Information.*

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of protected personal information in our possession and have taken precautions to safeguard it. We continually evaluate and modify our practices and controls to enhance the security and privacy of your personal information.

**If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted].** Representatives are available from 9 am - 9 pm Eastern Time, Monday through Friday, excluding holidays. This response line is staffed with professionals familiar with this incident and knowledgeable about what you can do to help protect against potential misuse of your information.

Sincerely,

Pennsylvania State Education Association

i

**– OTHER IMPORTANT INFORMATION –**

**1. Additional Details Regarding Your Credit Monitoring.**

**Website and Enrollment.** Scan the QR image or go to [redacted] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**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.

**Telephone.** Contact IDX at [redacted] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**2. Placing a Fraud Alert.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 90-day "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*** | ***Experian*** | ***TransUnion*** |
|---|---|---|
| P.O. Box 105069<br>Atlanta, GA 30348-5069<br>https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/<br>(800) 525-6285 | P.O. Box 9554<br>Allen, TX 75013<br>https://www.experian.com/fraud/center.html<br>(888) 397-3742 | Fraud Victim Assistance Department<br>P.O. Box 2000<br>Chester, PA 19016-2000<br>https://www.transunion.com/fraud-alerts<br>(800) 680-7289 |

**3. Consider 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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

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

In order to place the security freeze, you will 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 that 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 TTY: 1-866-653-4261, 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.

You may also reach out to the Social Security Administration to notify them of the impact on your Social Security Number. They may be reached by telephone at 1-800-772-1213 between 8:00 a.m. – 7:00 p.m. Eastern Time, Monday through Friday. If you are deaf or hard of hearing and use TTY equipment, you can call the TTY number at 1-800-325-0778.

## 6. State Specific Information.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.