

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

December 26, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: The Pennsylvania School for the Deaf– Incident Notification

To Whom It May Concern,

McDonald Hopkins PLC represents The Pennsylvania School for the Deaf (“PSD”). I am writing to provide notification of a ransomware incident that impacted PSD and may affect the security of personal information of approximately one (1) Maryland resident. PSD’s investigation is complete, however this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, PSD does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about July 10, 2023 the Pennsylvania School for the Deaf experienced a cybersecurity incident relating to its computer systems. Upon further analysis, PSD learned that they lost access to multiple files and or systems. PSD immediately engaged external cybersecurity professionals experienced in handling these types of incidents to restore their systems and conduct a thorough forensic investigation into the incident. PSD’s system is fully restored, and after a thorough forensic investigation, on December 19, 2023, PSD confirmed that a Maryland resident was impacted and located their most recent address. The impacted information for the resident included full name, Social Security number, medical information, and driver’s license number.

PSD has no indication that any information has been misused. Nevertheless, out of an abundance of caution, PSD wanted to inform you (and affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. PSD is providing the affected resident with written notification of this incident commencing on or about December 26, 2023, in substantially the same form as the letter attached hereto. PSD is advising the affected resident about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

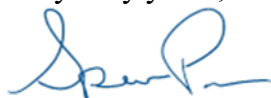
At PSD, protecting the privacy of personal information is a top priority. PSD is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. PSD continually evaluates and modifies its practices and internal controls to enhance the security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

December 26, 2023

Page 2

Should you have any questions regarding this notification, please contact me at (410) 917-5189 or spollock@mcdonaldhopkins.com.

Very truly yours,



Spencer S. Pollock

Encl. Sample Notification Letter



December 26, 2023

RE: NOTICE OF DATA SECURITY INCIDENT

Dear [REDACTED]:

We are writing to inform you of a data security incident at The Pennsylvania School For The Deaf (“PSD”) involving some of your information. 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?

On or about July 10, 2023 PSD experienced a cybersecurity incident that impacted connectivity to our network.

What We Are Doing

Upon experiencing the incident, PSD’s internal IT specialists took our networks offline to contain the threat and immediately commenced a prompt and thorough investigation. As part of our investigation, PSD has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation, PSD discovered on November 8, 2023 that on or around July 10, 2023, certain impacted files may have been removed from the PSD by an unauthorized individual.

What Information Was Involved?

The information potentially impacted by the unauthorized party included your name, date of birth, Social Security Number, driver’s license number, and medical information.

What You Can Do

We have no evidence that any personal information has been or will be used for identity theft or financial fraud as a direct result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

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. 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.

For More Information

Please accept our apologies that this incident occurred. We are 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 and internal 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] This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available for 90 days from the date of this letter, from 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

The Pennsylvania School For The Deaf

100 W School House Lane
Philadelphia, PA 19144
(215) 951-4700

– OTHER IMPORTANT INFORMATION –

1. Protecting Your Medical Information.

As a general matter, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12-month 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 30348-5069
<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

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(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

P.O. Box 105788
Atlanta, GA 30348-5788
<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.

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.