100 International Drive
23rd Floor
Baltimore, MD 21202

P 1.248.646.5070
F 1.248.646.5075

McDonald Hopkins
A business advisory and advocacy law firm®

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

September 5, 2023

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

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

Re: Deer Lakes School District - Cybersecurity Incident Notification

To Whom It May Concern:

We are writing on behalf of our client, Deer Lakes School District ("DLSD") (located at 19 East Union Road, Cheswick, PA 15024), to notify you of a cybersecurity incident involving two (2) Maryland residents. DLSD's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, DLSD does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature

On or about February 10, 2023, DLSD discovered that it was the victim of a ransomware incident that impacted its networks and servers. After discovering the incident, DLSD engaged our firm and third-party forensic and incident response experts to conduct a thorough investigation of the nature and scope of the incident and to assist in the remediation efforts.

DLSD recently concluded its initial investigation, which revealed that an unauthorized actor gained access to DLSD's network, via RDP, between January 22, 2023 and February 10, 2023, and, as a result, obtained some files. On August 29, 2023, after an extensive forensic investigation and document review, DLSD discovered that personal information was contained within the impacted files that were subject to unauthorized access or acquisition as a result of the incident. Further on August 31, 2023, DLSD located the most recent contact information for the individuals impacted. The personal information potentially obtained from the Maryland residents included first and last name and Social Security number.

Notice and DLSD's Response to the Event

On September 5, 2023, DLSD will mail a written notification to the potentially affected Maryland residents, pursuant to Md. Code Com. Law § 14-3504, in substantially similar form as the enclosed letter (attached as **Exhibit A**).

Additionally, DLSD is providing the potentially impacted residents the following:

- Free access to credit monitoring services for one year;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- 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 and law enforcement to report attempted or actual identity theft and fraud.

Further, DLSD will provide notice to the applicable government regulators, officials, and state Attorneys General (as necessary).

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 917-5189 or email me at spollock@mcdonaldhopkins.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

Exhibit A

Deer Lakes School District
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB07891 5-1

[redacted]

September 5, 2023

Important Information, Please Review Carefully

[redacted]

The privacy and security of the data we maintain is of the utmost importance to Deer Lakes School District ("DLSD"). We are writing with important information regarding a data security incident that involved some of your information. We want 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 February 10, 2023, DLSD became aware of potential unauthorized access to our network due to a cybersecurity incident.

What We Are Doing

Upon learning of this issue, we immediately contained the threat and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents.

We recently concluded our investigation and determined that an unauthorized actor infiltrated our network between January 22, 2023, and February 10, 2023, and, as a result, may have accessed or removed some data from our network. On August 29, 2023, after an extensive forensic investigation and manual document review, we discovered that certain personal information was contained within the impacted files that were subject to unauthorized access or acquisition as a result of the incident.

What Information Was Involved?

The impacted files contained some of your personal information, specifically your first and last name and Social Security number.

What You Can Do

To date, we are not aware of any reports of identity fraud or identity theft as a direct result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and 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 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in 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. For more information on identity theft prevention,

including instructions on how to activate your complimentary 12 months membership, please refer to the "Other Important Information" included with this letter.

This letter also includes 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 (if applicable) and credit reports for fraudulent or irregular activity. To the extent that is it helpful, we have included information about protecting you against medical identity theft.

For More Information

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. If you have any additional questions, please **call our dedicated and confidential toll-free response line that we have set up to respond to questions at** [redacted]. Please be prepared to supply the fraud specialist with your unique code listed below. 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, between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays.

Sincerely,

Dr. Janell Logue-Belden
Superintendent of Schools
Deer Lakes School District
19 East Union Road
Cheswick, PA 15024
724-265-5300

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12 months month Credit Monitoring.

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.

2. Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 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 can access the request form at https://www.annualcreditreport.com/index.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

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. 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

4. Consider Placing a Fraud Alert on Your Credit Report

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 twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

5. Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney

general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

6. Protecting Your Medical Information.

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.

7. Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, Telephone: 888-743-0023.