Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 21, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Events

To Whom It May Concern:

We represent Prince George's County Public School District ("PGCPS") located at 14201 School Lane Upper Marlboro, MD 20772, and are writing to notify your office of two recent, separate, incidents that may affect the security of certain personal information relating to a total of approximately one hundred eighty-three (183) Maryland residents. These incidents are not connected to the August 2023 data security incident previously reported to your office. The investigation into each matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PGCPS 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 of the Data Events

On February 1, 2024, PGCPS discovered suspicious activity involving an employee user account. Upon learning of this event, PGCPS promptly responded and launched an investigation with outside forensic specialists to confirm the nature and scope of the incident. The investigation discovered that a PGCPS employee had been accessing several PGCPS employee email accounts and PGCPS user accounts without authorization using their PGCPS usernames and passwords. The employee also accessed the Social Security number, driver's license information, and passport number of at least one employee without authorization to do so. The investigation into what other information may have been impacted is ongoing. We will supplement this notice further at the conclusion of the investigation to inform you of any additional data determined to be impacted by this incident.

On February 19, 2024, PGPCS discovered suspicious activity relating to several employee email accounts. The activity related to unauthorized access to PGCPS's identity management system which stored credentials for PGCPS email accounts. Upon learning of this event, PGCPS promptly responded and launched an investigation with outside forensic specialists to confirm the nature and scope of the incident. The investigation discovered that an unknown actor had accessed usernames and passwords for certain employees' email accounts without authorization and had been resetting PGCPS passwords and security questions to gain access to PGCPS email accounts. Upon discovery of this activity, PGCPS promptly took steps to secure the identity management system and secure impacted email accounts.

Notice to Maryland Residents

On or about March 21, 2024, PGCPS began providing written notice of these incidents to approximately one hundred eighty-three (183) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit A**.

Other Steps Taken and To Be Taken

Additionally, PGCPS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud. PGCPS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, 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, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security events described herein, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

EXHIBIT A

[redacted]

Dear Colleague,

I am writing to share information about your PGCPS email and user account password. We learned recently that an employee in PGCPS—not affiliated with the IT Division—gained access to the passwords of about 90 employees. Unfortunately, your password was among those compromised.

This password compromise is not at all related to the cyberattack from August 14, 2023. In fact, based on our investigation, it appears this employee had been attempting to cultivate passwords of colleagues—either by accessing someone's computer that was left open when an individual left their work station, or by offering to assist others who may have had computer troubles, thereby giving this employee access to someone else's computer where passwords may have been stored in the Google Chrome password manager. This employee was present at various central office facilities when large group trainings or events took place, allowing them the opportunity to gain access to the passwords of unsuspecting colleagues. As a reminder, please ensure to lock your computer when not at your desk and to not store passwords on your laptop or on post it notes that are readily accessible to others.

While the security investigation is ongoing, out of an abundance of caution I wanted to make you aware now that your passwords have been compromised. Although your PGCPS password was likely already changed in the course of routine password resets, I want to encourage you to reset your PGCPS password, and also encourage you to reset any personal passwords that you may have stored in your PGCPS Google Chrome password manager over the years, as this individual would have had visibility into this password manager tool using your PGCPS password. If we determine that other personal information relating to you may have been accessed by this individual, we will notify you directly as soon as practicable.

I am sure this news is very troubling, especially coming on the heels of the cyberattack last summer and subsequent data breach. Please know that as soon as we identified suspicious activity on the part of this employee, we immediately launched an investigation through an external cyber forensics firm to determine the scope of the impact and are notifying you now following the conclusion of that investigation.

Given the unique nature of this situation, where one of our own colleagues took advantage of others, I am particularly disheartened by this incident. I deeply regret that this incident has occurred, and I want to assure you that we continue to take steps to further enhance our overall network security, including the roll-out of Google 2-step verification right after spring break. We also encourage you to review the enclosed Steps You Can Take To Protect Personal Information for additional guidance.

I also want you to know that I am available to talk directly by phone with you about this situation if you have questions. Please do not hesitate to contact me directly and I will set up a time to talk with you.

Thank you.

Andrew Zuckerman, Chief Information Officer

301-952-620

Steps You Can Take To Protect Personal Information

Monitor Your Accounts

PGCPS advises you to remain vigilant against potential fraud by reviewing account statements and monitoring free credit reports. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

--
Andrew Zuckerman
Chief Information Officer
PGCPS