MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

February 16, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

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 write to notify your office of an incident that may affect the security of certain personal information relating to four (4) New Hampshire residents. This notice may 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 New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 14, 2023, PGCPS discovered certain systems had been encrypted with ransomware. Upon learning of this event, PGCPS immediately responded and launched an investigation with outside forensic specialists to confirm the nature and scope of the incident and restore impacted computer systems to operability. The investigation discovered that an unauthorized actor accessed PGCPS systems and likely viewed or acquired data containing certain information between August 3, 2023 and August 14, 2023. PGCPS then performed a comprehensive programmatic and manual review of the impacted data to determine whether it contained sensitive information. PGCPS recently concluded its review and determined on or around January 16, 2024, that personal information was included in the potentially impacted data set. Since this time, PGCPS has worked to locate current address information for the affected individuals, put resources in place to assist, and provide direct notice.

The information present in the files that may have been viewed or acquired as a result of this incident varies per person, and includes individuals'

Notice to New Hampshire Residents

On or about February 16, 2024, PGCPS began providing written notice of this incident to four (4) New Hampshire 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

Upon discovering the event, PGCPS moved quickly to investigate and respond to the incident, assess the security of PGCPS systems, and reset passwords for all user accounts. Further, PGCPS notified federal law enforcement regarding the event. Although there is no evidence of identity theft or fraudulent misuse of information in connection with this event, PGCPS is providing access to credit monitoring services for , through Experian, to individuals whose information was potentially affected by this incident, at no cost to these individuals.

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 to the appropriate institutions. 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.

PGCPS is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

EXHIBIT A

PGCPS
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 16, 2024

K8720-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF [SECURITY INCIDENT / DATA BREACH]

Dear Sample A. Sample:

Prince George's County Public Schools (PGCPS) writes to inform you of an incident that impacts the privacy of some of your information. We are providing you with notice of the incident, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so. You may be receiving this letter as a current or former student, employee, or prospective employee of PGCPS schools.

What Happened? As you may be aware, on August 14, 2023, we discovered a data security incident that impacted our computer systems and caused a temporary disruption to certain operations. We immediately responded and launched an investigation with outside forensic specialists to confirm the nature and scope of the incident and restore impacted computer systems to operability. The investigation discovered that in addition to usernames and passwords previously identified as impacted, that an unauthorized actor accessed our systems and likely viewed or acquired data containing certain information between August 3, 2023 and August 14, 2023. We then performed a comprehensive review of the impacted data to determine whether it contained sensitive information and to whom it relates. We recently concluded our review and determined on or around January 16, 2024, that information related to you was included in the potentially impacted data set. After determining the scope of information in the potentially impacted files, we undertook efforts to locate address information for the affected individuals, put resources in place to assist, and provide this direct notice.

What Information Was Involved? The information present in the files that may have been viewed or acquired as a result of this incident included your name and [data elements].

What We Are Doing. We treat our responsibility to safeguard the information entrusted to us as an utmost priority. As such, we responded immediately to this incident and have been working diligently to provide you with an accurate and complete notice of the incident. We have also implemented additional processes and procedures to help prevent similar incidents from occurring in the future.

As an added precaution, we are providing you with the opportunity to enroll in ## months of complimentary access to credit monitoring and identity restoration services through Experian IdentityWorks℠. Please note that if you have already enrolled in the credit monitoring service provided, re-enrolling will require setting up a separate profile. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included within the enclosure to this letter.

What You Can Do. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring and identity restoration services we are offering and how to enroll. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements regularly and monitoring your free credit reports for suspicious activity and to detect errors.

For More Information. We understand you may have questions about this incident. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at 833-918-1251, Monday through Friday 9 am – 11 pm EST, Saturday and Sunday 11 am – 8 pm EST (excluding major U.S. holidays).

Sincerely,

Andrew Zuckerman,
Chief Information Officer

Prince George's County Public Schools
Sasscer Administration Building
14201 School Lane
Upper Marlboro, MD 20772

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for ## months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at . Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

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/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 6 Rhode Island residents that may be impacted by this event.