Pulaski County Public Schools

202 N. Washington Avenue ❖ Pulaski, VA 24301 ❖ (540) 994-2519 ❖ (540) 994-2514 (fax)
Robert Graham, Division Superintendent

December 5, 2023
Via Certified Mail

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

Pursuant to New Hampshire Rev. Stat. § 359-C:20(I)(b), I am writing on behalf of Pulaski County Public Schools ("PCPS") to notify you regarding the nature and circumstances of a recent data security incident. PCPS's mailing address is 202 N. Washington Ave., Pulaski, VA 24301.

On November 5, 2023, the PCPS Department of Information Technology was alerted to suspicious activity affecting our network. We launched an immediate investigation to determine the nature and scope of the activity. As part of our response, PCPS engaged leading outside cybersecurity experts to investigate the nature and scope of this activity and remediate the incident. It quickly became apparent that PCPS was the victim of a ransomware attack.

In this matter, cybercriminals accessed servers in the PCPS environment and encrypted them. Fortunately, we successfully prevented the ransomware from compromising the physical security of our classrooms or otherwise disrupting the ongoing learning of our students. However, the cybercriminals claim to have removed certain data from our servers. Based on our investigation, there is a possibility that one or more of the following types of personal information could be implicated:

We have notified the FBI Cyber Crimes Division and the Virginia State Police's Fusion Intelligence Center of this attack. PCPS intends to support any law enforcement investigation into the incident. We have also arranged to provide potentially impacted individuals with of identity/credit monitoring and identity restoration services through Experian at no cost to them.

There is a single New Hampshire resident potentially impacted by this incident. For your reference, enclosed with this letter is a copy of the notification letter to be mailed on December 5, 2023, to the potentially impacted New Hampshire resident.

Please do not hesitate to contact me if you have any questions. You may also reach out to our outside counsel, Beth Burgin Waller, at Woods Rogers Vandeventer Black PLC, via email at

Sincerely,

Robert F. Graham
Superintendent
Pulaski County Public Schools

Enclosures

Pulaski County Public Schools
✦ (540) 994-2519 ✦ (540) 994-2514 (fax)
Robert Graham, Division Superintendent

c/o Experian
Return Mail Processing
PO Box 999
Suwanee, GA 30024

3618966 **********SNGLP
SAMPLE A. SAMPLE - L02
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

December 5, 2023

Dear Parents/Guardians of Sample A. Sample:

As previously communicated, earlier this month Pulaski County Public Schools ("PCPS") suffered a ransomware attack. We are writing to share with you how this incident may have affected your child's personal information and, as a precaution, to provide you with steps you can take to protect this information.

PCPS takes the privacy and security of your child's personal information very seriously and we sincerely regret any concern this incident may cause you.

What Happened

On November 5, 2023, the PCPS Department of Information Technology was alerted to suspicious activity affecting our network. We launched an immediate investigation to determine the nature and scope of the activity. As part of our response, PCPS engaged leading outside cybersecurity experts to investigate the nature and scope of this activity and remediate the incident. It quickly became apparent that PCPS was the victim of a ransomware attack.

Ransomware is a form of malware used by cybercriminals to prevent organizations from accessing files. In some cases, the criminals will extract and hold data hostage with aspirations of extorting a ransom. In this matter, a cybercriminal accessed servers in the PCPS environment and encrypted them. Fortunately, we successfully prevented the ransomware from compromising the physical security of our classrooms or otherwise disrupting the ongoing learning of our students. However, the cybercriminal claims to have removed some data from our servers.

What Information Was Involved?

There is a possibility that one or more of the following types of personal information could be implicated:

Out of an abundance of caution, we have arranged for free identity monitoring in addition to Experian's ID protection services, which are retroactive to the date of the incident. We are offering these services to all current PCPS students, and any former students with information potentially implicated by files the cybercriminal claims to have taken from PCPS servers. More information about the free identity monitoring services we are providing through Experian can be found in the attached Identity Theft and Protection Guide.

What We Are Doing

We have notified the FBI Cyber Crimes Division and the Virginia State Police's Fusion Intelligence Center of this attack. PCPS intends to support any law enforcement investigation into the incident. We take our obligation to safeguard personal information very seriously and are continuing to evaluate additional actions to strengthen our network security in the face of an ever-evolving cyber threat landscape.

What You Can Do

Please stay vigilant regarding your personal information and review the enclosed Identity Theft and Protection Guide for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary identity monitoring services being offered for your child through Experian *IdentityWorks*. Information regarding the identity monitoring enrollment is included in the attached Identity Theft and Protection Guide.

For More Information

If you have any further questions regarding this matter or the identity monitoring services provided, please call 833-603-7609 toll-free Monday through Friday 9 am – 11 pm Eastern, or Saturday and Sunday from 11 am – 8 pm Eastern (excluding major U.S. holidays). Please be prepared to provide your engagement number **B110287**. Please also note that PCPS is utilizing Experian's return mail service, so the return address on this letter is to their mailing center.

We deeply regret that this incident occurred and are committed to supporting you.

Sincerely,

Robert F. Graham
Superintendent
Pulaski County Public Schools

IDENTITY THEFT PROTECTION GUIDE AND INFORMATION

We encourage affected individuals to take the following steps:

Details Regarding Enrollment with Experian

To help protect your minor dependent's identity, we are offering complimentary access to Experian IdentityWorks[SM] for twelve months.

If you believe there was fraudulent use of your minor dependent's 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 twelve 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 membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your minor dependent's 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 as proof of eligibility for the Identity Restoration services by Experian.

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:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **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.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Obtain and Monitor Your Credit Report

As a precautionary measure, we recommend that you remain vigilant by regularly reviewing and monitoring account statements and credit reports to detect potential errors or fraud and identity theft resulting from the security incident. You may periodically obtain your free credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for inaccurate information, such as a home address and Social Security number. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Notify Law Enforcement of Suspicious Activity

You should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including local law enforcement, your state attorney general, and the Federal Trade Commission (FTC). To file a complaint with the FTC, use the below contact information or website.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.IdentityTheft.gov

Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company which the account is maintained.

Credit Freezes

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued when you initiate a freeze. A credit freeze is designed to prevent potential creditors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily

* 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.

lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact **all three** major consumer reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com/personal/credit-report-services	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Your full name, with middle initial and any suffixes;
2) Your Social Security number;
3) Your date of birth (month, day, and year);
4) Your current address and previous addresses for the past five (5) years;
5) A copy of your state-issued identification card (such as a state driver's license or military ID);
6) Proof of your current residential address (such as a current utility bill or account statement); and
7) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request. More information regarding credit freezes can be obtained from the FTC and the major consumer reporting agencies.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert will stay on your credit file one (1) year. The alert informs creditors of possible fraudulent activity within your report and requires the creditor to verify your identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the three major consumer reporting agencies listed above. The agency you contact will then contact the other two. More information regarding fraud alerts can be obtained from the FTC and the major consumer reporting agencies.

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number. You may want to order copies of your credit reports and check for any bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your records.

Additional Resources and Information

You can obtain additional information and further educate yourself regarding identity theft and the steps you can take to protect yourself by contacting your state attorney general or the FTC. The FTC's contact information and website for additional information is:

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

For Virginia residents: You may contact the Virginia Attorney General's Office at 202 North Ninth Street, Richmond, VA 23219; 1-804-786-2071; or https://www.oag.state.va.us/contact-us/contact-info.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General at 165 Capitol Avenue, Hartford, CT 06106; 1-860-808-5318; or https://portal.ct.gov/ag.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia at 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; or https://oag.dc.gov/consumer-protection/consumer-alert-online-privacy.

For Iowa residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at 1305 E. Walnut Street, Des Moines, IA 50319; 1-515-281-5164; or www.iowaattorneygeneral.gov.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 410-576-6300; 1-888-743-0023 (toll free), or https://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General at 1 Ashburton Place, Boston, MA 02108; 1-617-727-8400; or https://www.mass.gov/orgs/office-of-the-attorney-general. You have the right to obtain a police report if you are a victim of identity theft.

For New Mexico residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your credit file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit
https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or ww.ftc.gov.

For New York residents: The 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/. You may also contact the Bureau of Internet and Technology (BIT) at 28 Liberty Street, New York, NY 10005; 212-416-8433l; or https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology.

For North Carolina residents: The North Carolina Attorney General's Office may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 919-716-6400; or https://ncdoj.gov/contact-doj/.

For Oregon residents: We encourage you to report suspected identity theft to the Oregon Attorney General at 1162 Court Street NE, Salem, OR 97301; 1-877-877-9392; 1-503-378-4400; or www.doj.state.or.us.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or https://riag.ri.gov/. You have the right to obtain a police report if you are a victim of identity theft. Zero Rhode Island residents were impacted by this breach.