Pell City Schools
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS3543

0002793

13_0002793

April 14, 2025

Re: Notice of Security Incident

Dear :

I am writing to you about a cyber incident at Pell City Schools ("PCSS," "the District," "we," or "us") that involved some of your personally identifying information.

Importantly, our Human Resources and Student Information Systems (PowerSchool) were <u>not</u> affected by this incident.

At this time, we have no evidence that your information has been misused for identity theft or fraud. However, we are sending this letter to:

- Communicate what happened.
- Identify the personally identifying information involved.
- Provide details on how to enroll in twelve (12) months of free credit monitoring and theft resolution services.

What Happened? On December 10, 2025, we detected suspicious activity that we quickly determined was a cyber incident impacting some of the District's technology systems. Our security tools blocked much of this activity, but as a precaution we decided to take our computer systems offline to contain the incident. We also reported the incident to law enforcement and launched an investigation, working alongside cybersecurity experts.

The investigation determined that an unauthorized third party copied some of our files during the incident in an attempt to extort the District. We conducted an in-depth review of the files to understand what information was involved and recently learned that some of these files include your personally identifying information. This type of review takes time because we want to be accurate and avoid providing incomplete or incorrect information. We notified you as soon as possible once we learned your personally identifying information was involved.

What Information Was Involved? Our review located records that contained personally identifying information (as defined by state law), including your name, as well as electronic signature, date of birth, driver's license number, financial account number (without PIN or access code), medical information, passport number, and social security number.

What Are We Doing. In addition to the actions described above, we have taken steps to reinforce our technology systems by implementing additional security measures. We will continue to make investments to improve the District's resiliency.

What You Can Do. We have enclosed an *Identity Protection Reference Guide* to make you aware of ways to monitor and protect your personal information. We are also offering complimentary credit monitoring in case you would find it helpful to review your credit report. For more information on the Cyberscout services, including instructions on how to activate your complimentary twelve (12) months membership, please see the additional information provided in this letter.

For More Information. If you have any questions about this incident, or to activate the complimentary credit monitoring service, please reach out to our dedicated support team at from 7:00 am to 7:00 pm, CDT, Monday through Friday (excluding major U.S. holidays). For any other questions, please contact . Thank you for all you do for PCSS.

Sincerely,

Dr. Justin Burns
Superintendent

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax https://www.equifax.com/personal/credit-report-services/	Experian https://www.experian.com/help/	TransUnion 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

It is only necessary to contact <u>one</u> of these bureaus and use only <u>one</u> of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. You have a right to place a security freeze on their credit report. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. A security freeze must be requested in writing by certified mail or by electronic means as provided by a consumer reporting agency. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. When you place a security freeze on your credit report, you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a period of time after the freeze is in place.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

Alabama Residents: Any consumer in Alabama may place a security freeze on his or her credit report by making a request by mail to each consumer reporting agency. If the consumer reporting agency has procedures for accepting the request by phone, Internet, or fax, then the consumer may also use one of these methods to make the request. The consumer reporting agency may not charge a fee to consumers over 65 years of age or victims of identity theft. To avoid paying a fee, victims must send a valid investigative report, an incident report, or a complaint with a law enforcement agency about unlawful use of the victim's identifying information by another person. Individuals who are not over 65 years of age or who have not been victims of identity theft must pay a fee of no more than $10 per person, per consumer reporting agency, to place, temporarily lift, or remove a security freeze. A security freeze prohibits, with certain specific exceptions, the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer.

4. Request an IP PIN from the IRS. Although the IRS is capable of identifying suspicious tax returns, taxpayers may choose to take proactive steps to prevent fraud, including obtaining an Identity Protection PIN (IP PIN) from the IRS. The IP PIN is a 6-digit number that, when active, will be required to file a tax return using the taxpayer's SSN or ITIN. To request an IP PIN, visit https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

In addition, taxpayers may opt in to ID.me, an identity verification service that requires a photo ID or live video session before logging in to submit a tax return online.

Finally, taxpayers may submit IRS Form 14039, Identity Theft Affidavit online if they received IRS correspondence indicating they might be a victim of tax-related identity theft or if their e-file tax return was rejected as a duplicate. After submitting the form, the IRS will refer the taxpayer's case to the Identity Theft

Victim Assistance organization to investigate the case, remove fraudulent returns, and process the correct return and refund.

5. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider.

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

This notification was not delayed by law enforcement.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

Oregon Residents: You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-800-850-0228, https://www.doj.state.or.us/.

DETAILS REGARDING YOUR CYBERSCOUT MEMBERSHIP

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 twelve (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. 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, a TransUnion company specializing in fraud assistance and remediation services.

0002793

How do I enroll in the free services?

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: .

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.**