Lewis Central
Community School District

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

April 25, 2025

Subject: Notice of Data <<Variable Data 1>>

Dear << First Name>> << Last Name>>:

As you are likely aware, PowerSchool – a software vendor used by Lewis Central Community School District ("Lewis Central") – recently experienced a cybersecurity incident involving unauthorized acquisition of certain information stored in our Student Information System ("SIS"). The purpose of this letter is to notify you that the incident affected your personal information. Please read this letter carefully as it contains information about the incident and resources you can utilize to help protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On December 28, 2024, PowerSchool learned of a cybersecurity incident involving the unauthorized acquisition of certain personal information from PowerSchool SIS environments. On January 7, 2025, PowerSchool informed Lewis Central that our cloud-based SIS environment had been impacted. Upon notifying us of the incident, PowerSchool confirmed that it was contained and that there was no evidence of ongoing malicious activity. PowerSchool also stated that it had taken steps to protect the impacted data from further unauthorized access or misuse.

Since that time, we have been working diligently to identify and provide notice to individuals whose personal information was involved. Importantly, this incident occurred as a result of compromised PowerSchool credentials and impacted thousands of schools and school districts. This event occurred in the PowerSchool environment and did not impact the security of our computer systems in any way.

What Information Was Involved? The information involved included your name along with your <<Variable Data 2>>.

What We Are Doing. As soon as we discovered this incident, we took the steps referenced above. Importantly, PowerSchool is providing complimentary credit monitoring and identity theft protection services through Experian – a data breach and recovery services expert. These services include 24 months of credit monitoring, internet surveillance, identity restoration, Experian IdentityWorks ExtendCare™, and $1 Million Identity Theft Insurance.

To enroll, please follow the steps below:

- Ensure that you **enroll by** May 30, 2025 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/plus
- Provide your **activation code**: CTYU949PRK

If you have questions about the services, 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 833-918-9464. Be prepared to provide engagement number **B138812** as proof of eligibility.

What You Can Do. We encourage you to enroll in the Experian services PowerSchool is offering, which are at no cost to you. Please also review the guidance included with this letter which includes additional resources you may use to help protect your information.

For More Information. Representatives at Experian are available to assist you with enrolling in the services being offered and answer questions you may have regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Central Time, Monday through Friday, excluding holidays. Please call the call center toll-free at 833-918-9464 and provide the representative with your unique code listed above.

We apologize for the concern that PowerSchool's data security incident has caused.

Very truly yours,

Lewis Central Community School District
4121 Harry Langdon Blvd.
Council Bluffs, IA 51503

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: 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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

You also have certain rights under the Fair Credit Reporting Act ("FCRA"): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.