PowerSchool
Personalized Education for Every Journey

To: Involved NC PowerSchool SIS Customers

Dear PowerSchool SIS Customer,

Thank you for your continued patience and partnership as we address the recent cybersecurity incident. Over the last few weeks, we have been focused on assessing the scope of data involved, making further enhancements to our cybersecurity defenses, and developing a plan to help you and our shared community.

As a PowerSchool SIS customer whose information was involved, I am writing to provide you with updates on several important next steps:

Identity Protection and Credit Monitoring Services: PowerSchool has engaged Experian, a trusted credit reporting agency, to **offer complimentary identity protection and credit monitoring services** to all students and educators whose information from your PowerSchool SIS was involved. This offer is being provided regardless of whether an individual's Social Security number was exfiltrated.

- *Identity Protection:* PowerSchool will be offering **two years of complimentary identity protection services for all students and educators** whose information was involved.

- *Credit Monitoring:* PowerSchool **will also be offering two years of complimentary credit monitoring services for all adult students and educators** whose information was involved.

Notifications: Starting in the next few weeks, **PowerSchool will be handling notifications to involved individuals and relevant state attorney general offices on your behalf.** We hope to relieve the burden of these notifications on you and your institution.

- *Community:* PowerSchool will coordinate with Experian, to provide notice on your behalf to students (or their parents / guardians if the student is under 18) and educators, as applicable, whose information was involved, as well as a call center to answer questions from the community. The notice will include the identity protection and credit monitoring services offer (as applicable).

- *Regulatory:* PowerSchool will provide notification on your behalf to relevant state attorney general offices. You may also have notification requirements with your state's Department of Education where required. Since many customers have already notified and are in close contact with their state's Department of Education, PowerSchool will defer to you on these notifications.

In this communication, you will find a fact sheet with additional details on these steps and the incident, a template that we intend to use to notify individuals whose information was involved, and a proposed communication that you may choose to share with families and educators to

keep them informed on these steps. We are providing this communication package to technical contacts listed by your organization with PowerSchool. Please forward as appropriate to relevant leaders in your organization.

I sincerely value the trust you have placed in PowerSchool. We are committed to learning from this incident, becoming stronger and more resilient as a company for having experienced it – and most importantly – we are committed to serving you and our shared community.

We appreciate all that you are doing to support families and educators through this process.

Sincerely,
Hardeep Gulati
Chief Executive Officer, PowerSchool

PowerSchool
Personalized Education for Every Journey

PowerSchool Fact Sheet on Next Steps

Identity Protection and Credit Monitoring Services: PowerSchool will be offering two years of complimentary identity protection services for all students and educators whose information was exfiltrated from your PowerSchool SIS, which will also include two years of complimentary credit monitoring services for all adult students and educators whose information was involved, regardless of whether an individual's Social Security number was exfiltrated.

Experian, a trusted credit reporting agency, will be helping us to provide these services. Details on how to enroll will be included as part of individual notifications. As the offer is specific to this incident, the details contained in the forthcoming enrollment notification will be required to enroll, and cannot be obtained directly from Experian.

Credit monitoring agencies do not offer credit monitoring services for individuals under the age of 18. If a parent / guardian enrolls an individual under the age of 18 in the offered identity protection services, the individual, upon turning 18, will have the opportunity to enroll in credit monitoring services for the duration of the two-year coverage period.

Notifications: To reduce the burden of these notifications on you and your institution, **PowerSchool will be handling notification to individuals and state attorney general offices on your behalf.** You may have notification obligations to key stakeholders in our shared community.

- **Community:** In coordination with Experian, PowerSchool will provide notice on your behalf to students (or their parents / guardians for students under 18) and educators whose information was exfiltrated from your PowerSchool SIS.
    - PowerSchool will publish the notice on its website, circulate the notice to local media, and send the notice to email addresses, where available, of involved individuals.
    - The notice received by each individual will include a description of the categories of personal information that were exfiltrated and the identity protection and credit monitoring services offered (as applicable).
    - We will also provide you a link to the notification if you would like to share with your community.
    - Experian will also provide a call center to answer questions from the community.
- **Regulatory:** PowerSchool will provide notification on your behalf to relevant state attorney general offices. You may also have notification requirements with your state's Department of Education. Since many customers have already notified and are in close contact with their state's Department of Education, PowerSchool will defer to you on these notifications.
- For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of

birth, limited medical alert information, Social Security Number (SSN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base.

- **Timing:** PowerSchool intends to begin the notification process for relevant students, parents / guardians of students, educators, and state attorney general offices (as applicable) in the next few weeks.

We have also provided additional FAQs for North Carolina.

PowerSchool
Personalized Education for Every Journey

Proposed Update Communications

READY FOR DISTRIBUTION TO FAMILIES AND EDUCATORS
(PLEASE FEEL FREE TO CUSTOMIZE TO YOUR PREFERENCE)

TO: Our Community
FROM: [INSERT SCHOOL DISTRICT]
SUBJECT: An Update from [INSERT SCHOOL DISTRICT] on the PowerSchool Cybersecurity Incident

Email Body:

Dear families and educators of the [INSERT] community—

[As you may be aware / as we previously communicated], PowerSchool – a cloud-based software vendor used by [INSERT SCHOOL DISTRICT] – recently experienced a cybersecurity incident involving unauthorized access to certain information in the PowerSchool Student Information System (SIS).

We are reaching out to share more information and next steps that we recently received directly from PowerSchool:

- **Identity Protection and Credit Monitoring Services:** PowerSchool has engaged Experian, a trusted credit reporting agency, to offer **two years of complimentary identity protection services for all students and educators whose information from our PowerSchool SIS was involved. This offer will also include two years of complimentary credit monitoring services for all adult students and educators whose information was involved.**

- **Notification to Individuals Involved:** Starting in the next few weeks, in collaboration with Experian, PowerSchool will provide notice to students (or their parents / guardians if the student is under 18) and educators whose information was involved, as well as a phone number to answer any questions you may have about the incident. The notice will include the identity protection and credit monitoring services offer (as applicable).

- As soon as PowerSchool learned of the incident, they engaged cybersecurity response protocols and mobilized senior leadership and third-party cybersecurity experts to conduct a forensic investigation of the scope of the incident and to monitor for signs of information misuse. PowerSchool is not aware of any identity theft attributable to this incident.

In the meantime, I encourage you to visit https://www.powerschool.com/security/sis-incident/ for up-to-date information on the cybersecurity incident. We care deeply about the welfare of our [INSERT SCHOOL DISTRICT] families and will continue to do everything we can to support you. Thank you for the important role you play in our community and your shared commitment to putting our students first.

Sincerely,
[INSERT NAME]
[INSERT TITLE], [INSERT SCHOOL DISTRICT]

PowerSchool
Personalized Education for Every Journey

Form Individual Notification Template

DRAFT (VERISON NOT FOR DISTRIBUTION)

[Date of email notification]

DRAFT Notice of Data Breach

Dear PowerSchool User or Parent / Guardian of User:

As you may know, PowerSchool provides software and services to your current or former school or the current or former school of a person to whom you are a parent or guardian. We are writing to share with you some important information regarding a recent cybersecurity incident involving personal information belonging to you or to a person to whom you are a parent or guardian (the "individual").

What Happened? On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exportation of certain personal information from PowerSchool Student Information System (SIS) environments through one of our community-focused customer support portals, PowerSource.

What Information Was Involved? The types of information involved in this incident included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, and other related information. [The individual's Social Security number was also involved.] / [At this time, we do not have evidence that the individual's Social Security number was involved.]

What Are We Doing? PowerSchool is offering two years of complimentary identity protection services to students and educators whose information was involved. For adult students and educators, this offer will also include two years of complimentary credit monitoring services. If you are interested in enrolling, please sign up via [AAAAA] using the following code: [XXXXX] (if the individual is a minor) or [YYYY] (if the individual is an adult).

As soon as PowerSchool learned of the incident, we engaged cybersecurity response protocols and mobilized senior leadership and third-party cybersecurity experts to conduct a forensic investigation of the scope of the incident and to monitor for signs of information misuse. We are not aware of any identity theft attributable to this incident.

What Can You Do? You are encouraged to remain vigilant against incidents of identity theft and fraud by reviewing account statements for suspicious activity. PowerSchool will never contact you by phone or email to request your personal or account information. The enclosed "General Information About Identity Theft Protection" provides further information about what steps you can take.

Other Important Information. If you have any questions or concerns about this notice, please call [toll-free contact number], Monday through Friday between the hours of [9:00 am to 9:00 pm ET, excluding holidays].

Sincerely,

The PowerSchool Team

PowerSchool
Personalized Education for Every Journey

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

It is always advisable to regularly review statements from your accounts and periodically obtain your 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**, P.O. Box 740241, Atlanta, GA 30374-0241. 1.800.685.1111. www.equifax.com
- **Experian**, P.O. Box 9532, Allen, TX 75013. 1.888.397.3742. www.experian.com
- **TransUnion**, Consumer Disclosure Center, P.O. Box 1000, Chester, PA 19016. 1.800.888.4213. www.transunion.com

Fraud Alert: You may contact the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.888.378.4329
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

Security Freeze for Credit Reporting Agencies: You may request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. It is free to place, lift or remove a security freeze. You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

- **Equifax:** P.O. Box 105788, Atlanta, GA 30348, 1.888.298.0045, www.Equifax.com
- **Experian:** P.O. Box 9554, Allen, TX 75013, 1.888.397.3742, www.Experian.com
- **TransUnion:** P.O. Box 160, Woodlyn, PA 19094, 1.800.916.8800, www.TransUnion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years

- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies and include (1) proper identification; (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

You also have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your 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 http://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf or http://www.ftc.gov.

Steps You Can Take if You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

Additional Steps to Avoid Identity Theft: The FTC has further information about steps to take to avoid identity theft at: http://www.ftc.gov/idtheft; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State Specific Information

District of Columbia residents can obtain information from the District of Columbia's Attorney General's Office regarding steps to take to avoid identity theft. This office can be reached by visiting the website at https://oag.dc.gov/, calling (202) 727-3400, or visiting 400 6th Street NW Washington, D.C. 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at www.marylandattorneygeneral.gov, calling the Identity Theft Unit at 1.410.576.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

New York residents can learn more about preventing identity theft from the North York Office of the Attorney General, by visiting their web site at https://ag.ny.gov/resources/individuals/credit-lending/identity-theft, calling 1.800.771.77755 or requesting more information from the New York Attorney General's Office, 28 Liberty St, New York, NY 10005.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at https://ncdoj.gov/protecting-consumers/identity-theft/, calling 1.877.566.7226 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.401.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

South Carolina residents may access educational resources and the availability of consumer assistance from the South Caroline Department of Consumer Affairs. This office can be reached by visiting the website at https://consumer.sc.gov/, calling (803) 734-4200, or visiting 293 Greystone Boulevard, Ste. 400 Columbia, SC 29210.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.