ROPES & GRAY LLP
2099 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20006-6807
WWW.ROPESGRAY.COM

January 27, 2025

Edward McNicholas
T +1 202 508 4779
Edward.McNicholas@ropesgray.com

Attorney General Brenna Bird
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

Re: Data Incident

Dear Attorney General Bird:

We write on behalf of our client, PowerSchool, to inform you of a recent security incident that affected the personal information of approximately 49,921 Iowa residents.

On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration of certain personal information from PowerSchool Student Information System (SIS) environments through one of our community-focused customer support portals, PowerSource. The incident appears to have occurred between 12/19/2024-12/28/2024. This was not a ransomware event. No systems were encrypted and PowerSchool's operations and support for school districts in your state have continued uninterrupted.

The personal information at issue varies by individual (students, former students, and teachers) but includes some combination of the following for any given individual: the individual's name, contact information, social security number, date of birth, limited medical alert information, and other related information.

As soon as PowerSchool learned of the incident, it 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 has also reported the incident to law enforcement. We are not aware at this time of any identity theft attributable to this incident.

PowerSchool is supporting the notification process for school districts. A sample of the notifications that PowerSchool will provide is attached for reference. PowerSchool has engaged Experian to offer two years of complimentary identity protection and/or credit monitoring services to all students and educators whose information was involved. If you have any questions, please reach out to us at +1 (202) 508-4779.

Sincerely,

Edward R. McNicholas

Edward McNicholas

ROPES & GRAY LLP
2099 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20006-6807
WWW.ROPESGRAY.COM

Edward McNicholas
T +1 202 508 4779
Edward.McNicholas@ropesgray.com

January 27, 2025

Attorney General Brenna Bird
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

Re: Data Incident

Dear Attorney General Bird:

We write on behalf of our client, PowerSchool, which is a technology service provider to school district/school customers in your state, to provide additional context and details with respect to the recent security incident at PowerSchool described in a formal notification provided to you today. As described more fully in our formal notification, on December 28, 2024, PowerSchool became aware of a cybersecurity incident, which appears to have occurred between December 19 and December 28, 2024, pursuant to which personal information of state residents was exfiltrated. The personal information at issue varies by individual (students and teachers) but includes some combination for any given individual of name, date of birth, social security number, limited medical alert information, and contact information.

For the majority of its customers, PowerSchool hosted the data that was exfiltrated on PowerSchool's cloud environment ("hosted customers"). PowerSchool estimates that approximately 90 percent of its customers in your state are hosted customers. The remaining percentage of PowerSchool customers in your state maintain their data "on-premises," meaning those customers host the data on systems under their control ("on-prem customers"). The formal notification PowerSchool provided today was made on behalf of PowerSchool and its hosted customers who have not opted out of having PowerSchool provide this notice ("Covered Customers"). The number of state residents reported by PowerSchool is an approximated total of the data subjects for the Covered Customers which had information involved that triggers your state's data breach notification statute.

PowerSchool's notice excludes (a) hosted customers who have opted out and may determine to submit their own notifications and (b) "on-prem customers". Data subjects associated with on-prem customers are not included in PowerSchool's notice because PowerSchool does not have access to relevant data, which resides on those customers' internal systems. As a result, the information provided in today's formal

notification may not fully describe the extent of the data breach, but PowerSchool sought to provide timely reporting of information currently at its disposal. PowerSchool will either provide future notifications or support notification efforts that on-prem customers undertake, in each case as the customer determines that notification is necessary based on the evaluation of whether the exfiltrated on-prem customer data would require any such notification.

Sincerely,

Edward McNicholas

PowerSchool
Personalized Education for Every Journey

[Date of email notification]

Dear PowerSchool User or Parent / Guardian of User:

You are receiving this notice on behalf of [STUDENT OR TEACHER NAME] (the "named individual") from PowerSchool. 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. In compliance with State laws, we are writing to share with you some important information regarding a recent cybersecurity incident involving personal information belonging to the named individual.

What Happened? On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration 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? Due to differences in customer requirements, the types of information involved in this incident included one or more of the following, which varied by person: name, contact information, date of birth, Social Security Number, limited medical alert information, and other related information. At this time, we [do]/[do not] have evidence that the named individual's Social Security Number was involved. At this time, we [do]/[do not] have evidence that limited medical alert information for the named individual 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 whose information was involved, this offer will also include two years of complimentary credit monitoring services.

If your personal information was involved in this incident and you are interested in enrolling in credit monitoring or identity protection, please follow the steps for either Option 1 or Option 2 below:

Option 1: If the Named Individual is 18 or Over

Enrollment Instructions

- Ensure that you **enroll by** [Enrollment End Date] (Your code will not work after this date at 5:59 UTC)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]
- For over the phone assistance with enrollment or questions about the product, please contact Experian's customer care team at [Experian TFN]
- Be prepared to provide engagement number [B######]
- Experian's call center hours are Monday through Friday, 8:00am through 8:00pm Central Time (excluding major US holidays)

Details Regarding Your Experian Identityworks Credit Plus 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.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **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.

Option 2: If the Named Individual is Under 18

Enrollment Instructions

- Ensure that you **enroll by** [Enrollment End Date] (Your code will not work after this date at 5:59 UTC)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]
- For over the phone assistance with enrollment or questions about the product, please contact Experian's customer care team at [Experian TFN]
- Be prepared to provide engagement number [B######]
- Experian's call center hours are Monday through Friday, 8:00am through 8:00pm Central Time (excluding major US holidays)

Details Regarding Your Experian Identityworks Minor Plus 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:

- **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.

* 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.

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 at this time 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 [Experian TFN], Monday through Friday, 8:00am through 8:00pm Central Time (excluding major US holidays).

Sincerely,
The PowerSchool Team

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.