West Ada
SCHOOL DISTRICT

January 11, 2025

Via Email: consumer_protection@ag.idaho.gov

Attorney General Raul Labrador
Office of the Idaho Attorney General
Consumer Protection Division 954 W. Jefferson, 2nd
Boise, ID 83702

RE: Breach of PowerSchool Student Information Systems Database

Dear Attorney General Labrador:

Pursuant to Idaho Code § 28-51-105, which mandates prompt notification to the Attorney General following a data breach affecting personal information, I am notifying you of a breach involving the West Ada School District's PowerSchool Student Information System. This notification is provided within the required timeframe and follows verbal confirmation from your office on January 9, 2025.

Nature of the Incident

On January 7, 2025, PowerSchool Group LLC informed the West Ada School District of a cybersecurity incident affecting the PowerSchool support platform, PowerSource. According to PowerSchool, the breach occurred between December 19, 2024, and December 23, 2024, and involved unauthorized access to customers' PowerSchool Student Information System (SIS) databases.

PowerSchool Group LLC became aware of the breach on December 28, 2024, and subsequently informed districts of the incident. The breach involved the use of compromised credentials (username and password) to access PowerSource. A threat actor used tools within the support platform to connect to and extract data from SIS databases nationwide.

When PowerSchool detected the breach, they notified law enforcement, locked down the affected systems, and engaged the services of cybersecurity firms CrowdStrike and CyberSteward. PowerSchool has stated that they paid the threat actor not to release or disseminate the compromised data and received "reasonable assurances" from the threat actor that the data has

been deleted and no additional copies exist. PowerSchool, along with its third-party cybersecurity contractors, continues to monitor the web for any evidence of data release.

West Ada School District Response

The West Ada School District acted swiftly upon notification of the breach:

1. **Immediate Communication**: On January 9, 2025, we issued an initial notification to current West Ada employees and student families via email.
2. **Technical Mitigation**: The District's Technology Department attended multiple meetings with PowerSchool Group LLC. We have disabled support connections between PowerSource and all PowerSchool Student Information System product instances.
3. **Security Enhancements**: We are actively assessing our environment for security improvements as additional technical details concerning this breach become available.
4. **Data Analysis**: The District has begun analyzing the data involved in the breach to proactively notify affected parties and validate PowerSchool's findings.
5. **External Consultation**: We are consulting with external cybersecurity experts to strengthen our security posture and ensure compliance with best practices and legal requirements.

Categories of Data Affected

Preliminary information from PowerSchool Group LLC and our internal review indicates that the breach may have exposed Personally Identifiable Information (PII) as defined by Idaho Code § 28-51-104 and Idaho Code § 33-133. This may include the following:

- Names, addresses, and contact information for current and past students and staff;
- Life-safety, health, and grade information for current and former students;
- Parent/guardian/emergency contact names and addresses for current and past students.

While PowerSchool's investigation is ongoing, the District estimates that over 149,000 student records may have been affected. We are also reviewing whether this breach includes data protected under FERPA or other federal statutes.

Legal and Regulatory Compliance

The West Ada School District is taking all necessary steps to comply with Idaho Code § 28-51-105(1) and other applicable laws. Formal notifications are being prepared for all affected individuals, and we are evaluating the provision of credit monitoring services or other protective measures to mitigate potential harm.

We respectfully request your office's guidance on any additional actions required to ensure compliance with Idaho law and safeguard affected individuals' information. Additionally, we seek confirmation of any further steps your office recommends to address this incident.

Attachments and Supporting Documents

For your convenience, we have attached relevant supporting documents, including:

- A timeline of events;
- Correspondence from PowerSchool Group LLC;

Contact Information

West Ada School District is committed to protecting the data of our students, staff, and families. We will continue communicating transparently about this incident as new information becomes available. Concerned parties should submit a support ticket to our incident response team through our online system West Ada Technology Support Ticket.

Thank you for your attention to this matter. Please do not hesitate to contact me directly for further information or clarification.

Sincerely,

Devan DeLashmutt
West Ada School District
Chief Technology Officer
Delashmutt.devan@westada.org
208-350-5151

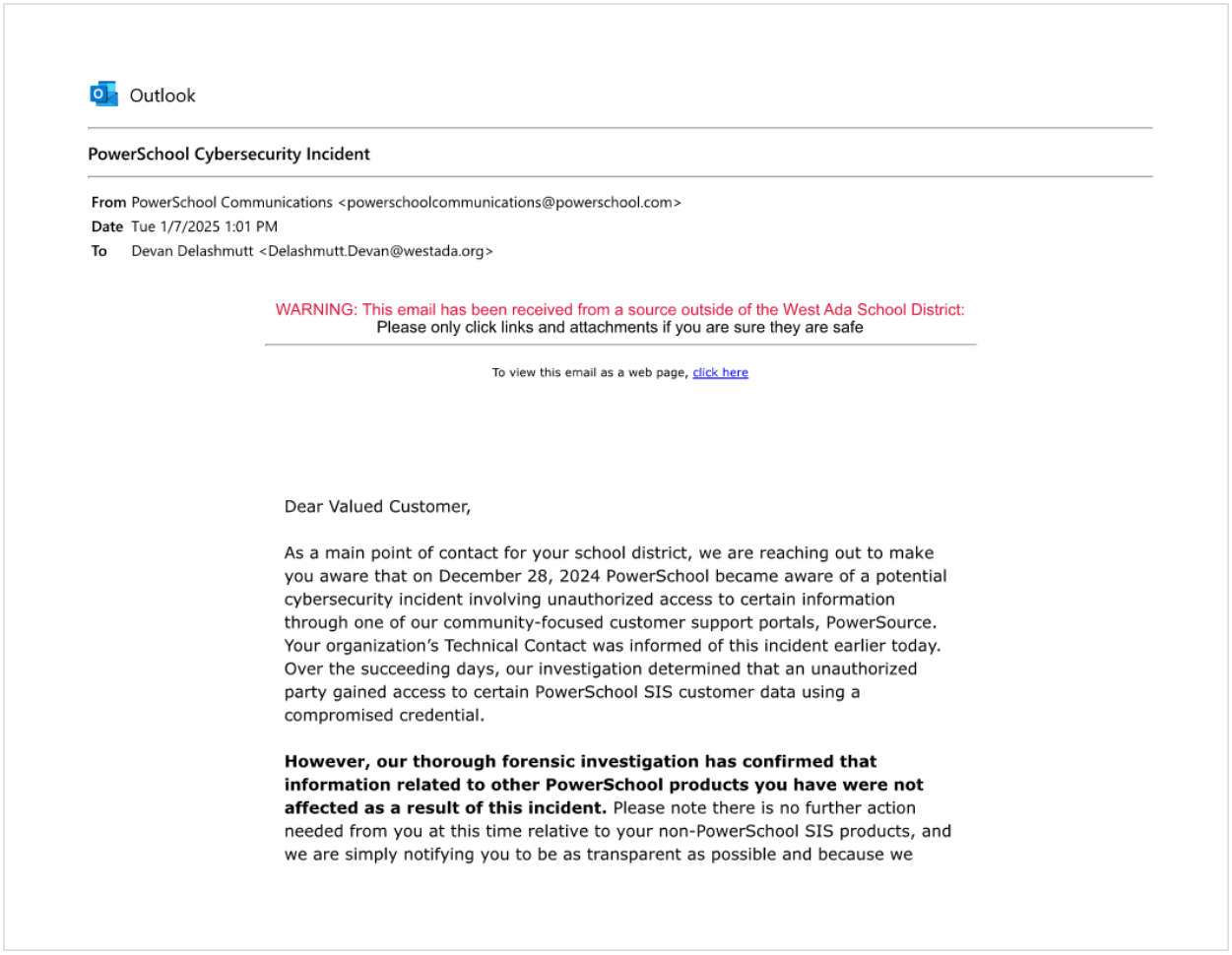
Attachments and Supporting Documents

PowerSchool Data Breach Timeline

Date Time	*Event*
January 7, 2025, 11:50A	PowerSchool Notification #1 Received
January 7, 2025	PowerSchool Notification #2 Received
January 8, 2024, 1:00P	PowerSchool Group LLC, Technical Briefing #1
January 8, 2024, 2:00P	West Ada Incident Response Team activated Formal Internal Investigation begins
January 8, 2025	Notification of Potential Data Breach • Phone call to Idaho Attorney General's Office
January 8, 2025, 4:36P	E-mail Notification of Potential Data Breach – SBOE and SDE • Executive Director of the State Board of Education • State Superintendent of Public Instruction
January 9, 2025	West Ada Incident Response Team: Investigation Continues
January 9, 2025, 12:00p	Data Breach Notification sent to current families and staff
January 9, 2025, 1:24p	Notification of Potential Data Breach Return phone call from State Attorney General's Office • Guidance confirms Data Breach Notification Protocol
January 9, 2025, 3:05P	Notification sent to District Insurance Company
January 9, 2025, 2:30P	PowerSchool Technical Briefing #2 Confirmation of Data Breach
January 10, 2025	West Ada Incident Response Team: Investigation Continues
January 11, 2025	West Ada Notification to Idaho Attorney General
January 11, 2025	Investigation Ongoing

PowerSchool Notification #1

PowerSchool Notification #2



Outlook

PowerSchool Cybersecurity Incident

From PowerSchool Communications <powerschoolcommunications@powerschool.com>
Date Tue 1/7/2025 1:01 PM
To Devan Delashmutt <Delashmutt.Devan@westada.org>

WARNING: This email has been received from a source outside of the West Ada School District:
Please only click links and attachments if you are sure they are safe

To view this email as a web page, click here

Dear Valued Customer,

As a main point of contact for your school district, we are reaching out to make you aware that on December 28, 2024 PowerSchool became aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Your organization's Technical Contact was informed of this incident earlier today. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool SIS customer data using a compromised credential.

However, our thorough forensic investigation has confirmed that information related to other PowerSchool products you have were not affected as a result of this incident. Please note there is no further action needed from you at this time relative to your non-PowerSchool SIS products, and we are simply notifying you to be as transparent as possible and because we

value our partnership with you. We have already notified technical contacts responsible for PowerSchool SIS in your organization.

As soon as we learned of the incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We have also informed law enforcement.

We have also deactivated the compromised credential and restricted all access to the affected portal. Lastly, we have conducted a full password reset and further tightened password and access control for all PowerSource customer support portal accounts.

Importantly, the incident is contained, and we have no evidence of malware of continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor expects to experience any operational disruption and continues to provide services as normal to our customers.

We are addressing the situation in an organized and thorough manner, following all of our incident response protocols. PowerSchool is committed to providing affected customers with the resources and support they may need as we work through this together.

Again, although your product was not impacted, we wanted to assure you that we are addressing the situation in an organized and thorough manner following all of our incident response protocols. Should you have any questions, please do not hesitate to contact your customer service manager. Thank you for your continued support and partnership.

Best,
Hardeep Gulati
Chief Executive Officer

Paul Brook
Chief Customer Officer

cc: **Mishka McCowan**