BONNEVILLE
JOINT SCHOOL DISTRICT NO. 93
Designing Success for Every Student

3497 North Ammon Road, Idaho Falls, Idaho, 83401 ★ (208) 525-4400 ★ Fax (208) 557-6800 ★ www.d93schools.org

Dr. Scott Woolstenhulme, Superintendent

Wednesday, January 8th, 2025

Attorney General's Office
Consumer Protection Division
P.O. Box 83720
Boise, ID 83720-0010

Re: PowerSchool Cybersecurity Incident

Dear Office of the Attorney General:

I am writing to notify you that Bonneville Joint School District 93 has experienced a data breach that resulted in some student and teacher personal information from our student information system (SIS) being compromised.

On Monday, January 6th, our IT department was notified by PowerSchool, our SIS provider, "that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed." Following this notification, our IT staff reviewed data access logs and found that this party had accessed data from two tables in our SIS, the Student table and the Teacher table. The records contained in these tables can be viewed at the following link: https://d93.org/powerschoolbreach.

On Wednesday, January 8th, we received a more in depth briefing from PowerSchool cyber security officials. In that briefing, they confirmed that only data from those two tables had been taken from affected school districts across the country and globe. They further stated that they had engaged the firms CyberSteward and CrowdStrike to investigate and respond to the cybersecurity attack. That response included engaging with the party who breached their system and negotiating an agreement through which the party destroyed the stolen data.

On the afternoon of January 8th, we notified our current employees and student families of the data breach by sending this statement to them via email, text message, and app notification: https://d93.org/breach. We will send this notification to the other email addresses and phone numbers that were stored in the SIS by the end of the week.

We have closed the back channel connection between our servers and the PowerSchool IT team and will only open that channel on an as needed basis for a limited amount of time. We are also reviewing other on-premise servers that house personal information to ensure other such connections are not kept open. At this time, based on the information and recommendations provided to us by the PowerSchool officials, we believe that there is no ongoing threat related to this security breach.

Sincerely,

Dr. Scott G Woolstenhulme
Superintendent of Schools
Bonneville Joint School District 93

BONNEVILLE
JOINT SCHOOL DISTRICT NO. 93
Designing Success for Every Student

3497 North Ammon Road, Idaho Falls, Idaho, 83401 ★ (208) 525-4400 ★ Fax (208) 557-6800 ★ www.d93schools.org

Dr. Scott Woolstenhulme, Superintendent

January 8, 2025

Dear D93 Families and Employees,

Yesterday afternoon, PowerSchool notified our IT Department that Bonneville School District 93 was affected by a cybersecurity incident that occurred on December 22nd. According to PowerSchool, an unauthorized individual used a compromised credential to access their system. The threat actor then used maintenance access channels to access data stored on the school district's PowerSchool servers. Upon discovering the incident, PowerSchool notified law enforcement, locked down the system, and engaged CyberSteward and CrowdStrike to investigate and respond to the cybersecurity attack.

Once we were notified of this incident by PowerSchool, the District 93 IT Team investigated access logs for PowerSchool and confirmed that the threat actor did in fact steal data from the Students table and the Teachers table in our PowerSchool database. These tables included records of students and teachers dating back to 2005. The personally identifiable information (PII) that was stolen was primarily limited to names, home addresses, phone numbers, and email addresses. It is important to know that we do not keep any social security numbers for students and social security numbers for teachers are only kept in School ERP, our secure employee information system. To see all of the fields that are included in these tables, please go to d93.org/powerschoolbreach.

In a webinar today, security officials from PowerSchool assured us that they have worked with the threat actor to ensure that all stolen records have subsequently been destroyed.

Although this incident originated with PowerSchool, we take this situation very seriously. Out of an abundance of caution, we are actively taking the following steps:

- We have disabled the PowerSchool remote support option.
- We have blocked IP addresses from the country where this attack originated as well as other countries where these types of attacks typically originate from.
- We have reported this incident to the Idaho Counties Risk Management Pool and will coordinate with them on engaging further cybersecurity support.

We expect PowerSchool to provide impacted individuals with additional resources, which we will post to d93.org/powerschoolbreach as soon as they become available.

At Bonneville School District 93, we are committed to safeguarding the data of our students, staff, and families. We will continue to communicate openly and transparently as we address this matter. If you have any questions or believe your information may have been compromised, please contact Gordon Howard at (208) 525- 4493.

Sincerely,

Dr. Scott Woolstenhulme
Superintendent
Bonneville School District 93

PowerSchool

Dear Valued Customer,

As the Technical Contact for your district or school, we are reaching out to inform you that on December 28, 2024, PowerSchool become aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed.

Please review the following information and be sure to share this with relevant security individuals at your organization.

As soon as we learned of the potential 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 can confirm that the information accessed belongs to certain SIS customers and relates to families and educators, including those from your organization. The unauthorized access point was isolated to our PowerSource portal. As the PowerSource portal only permits access to the SIS database, **we can confirm no other PowerSchool products were affected as a result of this incident**.

Importantly, the incident is contained, and we have no evidence of malware or 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.

Rest assured, we have taken all appropriate steps to prevent the data involved from further unauthorized access or misuse. We do not anticipate the data being shared or made public, and we believe it has been deleted without any further replication or dissemination.

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.

PowerSchool is committed to working diligently with customers to communicate with your educators, families, and other stakeholders. We are equipped to conduct a thorough notification process to all impacted individuals. Over the coming weeks, we ask for your patience and collaboration as we work through the details of this notification process.

We have taken all appropriate steps to further prevent the exposure of information affected by this incident. While we are unaware of and do not expect any actual or attempted misuse of personal information or any financial harm to impacted individuals as a result of this incident, PowerSchool will be providing credit monitoring to affected adults and identity protection services to affected minors in accordance with regulatory and contractual obligations. The particular information compromised will vary by impacted customer. We anticipate that only a subset of impacted customers will have notification obligations.

In the coming days, we will provide you with a communications package to support you in engaging with families, teachers and other stakeholders about this incident. The communications package will include tailored outreach emails, talking points, and a robust FAQ so that district and school leadership can confidently discuss this incident with your community.

We understand that you may have additional questions as a result of this update. FAQs are available on PowerSchool Community. Additionally, we will be holding webinars with senior leaders, including our Chief Information Security Officer, to address additional concerns. Please click the link below to register for a webinar that fits your schedule. Note that content for all sessions will be identical, so you need only attend one.

Wednesday, January 8: REGISTER HERE

Thursday, January 9: REGISTER HERE

In the meantime, please reach out to your Customer Success Manager (CSM), Support, or other established PowerSchool contact should you have any questions. We will be sending communications later today to other stakeholders in your organization who are responsible for other PowerSchool products notifying them of no impact to the other PowerSchool products.

We are addressing the situation in an organized and thorough manner, and we are committed to providing affected customers with the resources and support they may need as we work through this together.

Thank you for your continued support and partnership.

Sincerely,
Hardeep Gulati
Chief Executive Officer

Paul Brook
Chief Customer Officer

cc: **Mishka McCowan**
Chief Information Security Officer

PowerSchool •