Dear Valued Customer,

On January 7th, we shared that PowerSchool was the target of a cybersecurity incident that resulted in the exfiltration of data from the Students and Teachers tables for some PowerSchool SIS customers by an unauthorized user. We immediately took corrective measures necessary to contain the incident, began notifying relevant regulatory agencies on your behalf (where applicable) as well as students and educators whose data was involved, and provided credit and identity monitoring services to the individuals students and educators.

Today we are sharing closing updates on:

1. The final CrowdStrike Incident Report, which did not identify any new or concerning findings beyond what we have shared;
2. Our ongoing engagement with regulators in the United States and Canada;
3. The identity monitoring (and credit monitoring, as applicable) that PowerSchool continues to make available to all individuals involved, and
4. How PowerSchool has and will continue to strengthen our cybersecurity defenses as we connect the education community with the shared goal of helping students thrive through personalized education.

CrowdStrike Incident Report

Immediately after PowerSchool became aware of the incident, CrowdStrike was engaged to conduct an investigation into the incident. We made available a CrowdStrike interim fact sheet in mid-January, and with the investigation complete, are now sharing the final incident report.

CrowdStrike did not identify any new or concerning findings beyond what we already shared in the interim fact sheet. The report confirms:

- The Threat Actor accessed PowerSource, a community-focused customer support portal, using a single compromised credential.
- The Threat Actor's activities were limited to exfiltration of select PowerSchool SIS instances of Students and Teachers tables.
- CrowdStrike's Recon+ Intelligence service has not identified any evidence of this exfiltrated information available for sale or download.
- CrowdStrike found no evidence of system-layer access or malware associated with this incident.
- CrowdStrike found no other PowerSchool products were compromised.
- While the PowerSource environment experienced unauthorized activity prior to December, PowerSchool believes that the data exfiltration occurred in late December.

In addition to sharing here, we are posting CrowdStrike's final incident report on our website and sharing it with regulators in the United States and Canada where appropriate. We encourage you to share this report with any stakeholders that you deem appropriate.

Regulator Notifications – United States & Canada

As we shared on January 27th and February 4th, PowerSchool filed notifications with applicable regulators across U.S. and Canadian jurisdictions (respectively) on behalf of impacted customers who did not opt out of our offer to do so. Our dialogue with regulators is ongoing. We plan to share the final CrowdStrike incident report and additional relevant details from our on-premise customers who opted to share their information with us.

Identity & Credit Monitoring Notifications

On January 17th, we announced that PowerSchool secured two years of complimentary identity protection for all students and educators involved where such services are available through Experian, regardless of whether an individual's social security number was exfiltrated. We also made available two years of credit monitoring for involved students and educators in the United States and Canada who are eligible for credit monitoring services. To further support your communities with these resources, please note:

- Experian, our identity protection services provider, has sent email notifications on PowerSchool's behalf (except those customer who opted out) to both current and former families and educators whose information was involved, and for whom we have available contact information. These notifications will continue as we process on-premise customer information.
- These individual notices are sent from an Experian company, CSIdentity whose domain includes **@csid**. Please contact your CSM or Support team leader if you have any questions. Neither PowerSchool nor Experian will ever ask you for personal information via email.
- You can share information regarding the available monitoring services to your communities using the form letters provided to you by PowerSchool or the information provided on PowerSchool's website.
- Information on how to enroll in identity and credit monitoring is posted on PowerSchool's website (for the U.S. and Canada). We encourage you and your communities to take advantage of the monitoring being offered.
- PowerSchool has **extended the sign-up deadline** for Experian's services from May 31, 2025, to **July 31, 2025**.

Security Improvements and Hardening Measures Introduced

As part of our commitment to continuously strengthen security across the K-12 ecosystem, PowerSchool has taken significant steps to enhance our cybersecurity posture. To-date we have:

- Required that 100% of PowerSchool employees and contractors utilize SSO, MFA, VPN, and VDI for any hardware or resource that accesses customer data – including PowerSource;
- Invested in physical security measures including fingerprint and facial recognition authentication for all PowerSchool employees and contractors;
- Implemented rigorous technical audits of all access to customer data to validate and reinforce our security framework, including shortening the time-windows for authorized maintenance to reduce the risk of improper access; and,
- Limited the number of SIS instances a single account can log into during a 24-hour period.

In addition, we have taken proactive measures to reinforce our unwavering commitment to safeguarding student and educator data, including:

- Establishing a new Customer Security Advisory Council, which will provide a forum for in-depth security reviews, industry collaboration, and best practice sharing.
- Developing a security rubric to help districts assess not only PowerSchool's security commitment but also their own infrastructure and third-party systems.
- Continuing our long-standing security protocols, including adherence to global standards (such as ISO 27100), product-level governance (including SOC II audits), and monitoring via our Security Operations Center, which currently maintains 24x7x365 coverage against cybersecurity threats. You can learn more about our security process and policies here.

We hope this update can begin to bring closure to this incident; please reach out to your CSM or Support contact with any additional questions or concerns. We are grateful for your partnership over the last several weeks and look forward to all that we can accomplish as we move forward—together.

Sincerely,
Hardeep Gulati
Chief Executive Officer, PowerSchool