United States Senate

WASHINGTON, DC 20510

February 21, 2025

Hardeep Gulati
Chief Executive Officer
PowerSchool
150 Parkshore Drive
Folsom, CA 95630

Michael Ward
Chief Operating Officer
Bain Capital
200 Clarendon Street
Boston, MA 02116

Dear Mr. Gulati and Mr. Ward:

We write to express significant concern about the risks that students, staff, and school districts face after malicious actors stole their personal data in a cyberattack on your company's information systems. We urge PowerSchool to immediately notify all students and staff whose personal data may have been compromised, provide impacted individuals with identity protection services free-of-charge as soon as possible, and provide answers to questions regarding your company's reported cybersecurity failings.

More than 16,000 customers use PowerSchool's software products to serve 50 million students in the United States.[1] Schools use PowerSchool's Student Information System (SIS) service to manage student enrollment, attendance, grades, and records - as well as school staff records. These records could include dates of birth, Social Security numbers, home addresses, health information, and other private, personally identifiable information.

According to recent reports, malicious actors breached PowerSchool's SIS service and stole this sensitive data, putting students and staff at significant risk of identity theft. School district leaders who we have spoken with raised serious concerns about delays in your company's response to the cybersecurity incident, including delayed notifications to impacted schools. While the breach occurred as early as December 19, 2024, you failed to detect it until December 28, 2024.[2] Moreover, you did not notify SIS customers of the incident until January 7, 2025 – nineteen days after the incident.

Your company also has not clearly communicated a date by which impacted individuals will receive free identity protection and credit monitoring services. Your delayed and unclear communication is unacceptable, especially given the sensitive nature of the personal data that was stolen. We urge you to immediately notify all impacted individuals and provide them with these protective services.

According to reports, your company failed to put in place basic cybersecurity safeguards– such as multi-factor authentication – that could have helped to prevent the cyberbreach. Moreover, since the cybersecurity incident, PowerSchool has reportedly hired a cybersecurity technology company to conduct an analysis of the incident. This is an important step toward accountability and regaining the trust of your customers and the public. We ask you to be transparent with the

---

[1] Education Week, "What Schools Should Know About the PowerSchool Data Breach." January 9, 2025. https://www.edweek.org/technology/what-schools-should-know-about-the-powerschool-data-breach/2025/01

[2] PowerSchool landing page, https://www.powerschool.com/security/sis-incident/. Accessed January 30, 2025.

analyst's findings, and we request your prompt and comprehensive answers to the following questions:

1. Please detail the timeline of events from the date that the SIS cybersecurity incident occurred through today.
2. How many individuals across the United States had their data compromised by the December 2024 cyberattack on SIS? Please provide a breakdown of the number of current and former students and school staff who were impacted by state and school district.
3. What assistance have you provided to states, school districts, and schools that were impacted by the data breach, and what supports will you provide them moving forward?
4. How far back do the compromised records go? For instance, if a school used SIS services 10 years ago but no longer does, was that school impacted by the breach?
5. What assistance have you provided to states, school districts, and schools that no longer have an active SIS contract but are past clients and whose data was compromised?
6. Schools may use several PowerSchool software products. Were any of your other software products compromised by the cybersecurity incident? If so, was student and staff data accessed, and what are your plans to notify and support impacted individuals?
7. Please provide a date by which your company will fulfill its stated commitment to provide two years of complimentary identity protection and credit monitoring services to students and staff whose personally identifiable information was compromised. Do you commit to providing these services to all impacted students and staff even if it is not required by state law or your contracts? Did your company require multi-factor authentication for PowerSchool employees and contractors at the time of the breach? If not, why, and will you commit to requiring the use of this cybersecurity safeguard moving forward?
8. How swiftly did you notify federal, state, and local law enforcement about the cybersecurity incident, and are you cooperating with any investigations they may have underway into the incident?

Thank you for your attention to this important matter. We ask that you reply no later than March 7, 2025.

Sincerely,

Margaret Wood Hassan
United States Senator

Jim Banks
United States Senator

James Lankford
United States Senator