How Schools Should Respond to the PowerSchool Cyberattack

Insights
1.10.25

The country's largest provider of cloud-based education software for K-12 schools announced on January 7 that it fell victim to a massive data breach – which may lead to questions about the implications for your school. PowerSchool – which manages student records, grades, attendance, and enrollment for thousands of schools and over 50 million students – said it became aware of the incident on December 28 and took steps that it believes led to the stolen data being deleted. But even if the immediate threat is over, what steps should you, or must you, take to protect your school and prepare yourself for potential questions from your school community?

What happened?

According to PowerSchool, cyberattackers accessed "sensitive personal information" during a December data breach. The hackers broke into the software company's internal customer support portal using a stolen credential and accessed:

- For **students and teachers**: contact details (names and addresses), Social Security numbers, some medical and grade information, and other personally identifiable information (PII).
- For **parents and guardians**: some names, phone numbers, and email addresses could have also been accessed.

The information compromised will vary from school to school.

Will the data become public?

PowerSchool announced that it had worked with a cyber-extortion incident response service to negotiate with the cybercriminals and pay a ransom to resolve the matter. The software company said it had "taken all appropriate steps" to prevent the data from being misused and "does not anticipate the data being shared or made public." It concluded: "PowerSchool believes the data has been deleted without any further replication or dissemination."

What's next?

PowerSchool said it will work to identify all impacted schools and individuals in the coming weeks – and then follow the required notification process for all those impacted. It announced that it will offer all affected adults free credit monitoring and provide identity protection services to affected

minors, as required by law or contractual obligation. PowerSchool also said it will release a full report about the incident at the conclusion of its own internal investigation, expected by January 17.

What can we expect?

PowerSchool indicated it will provide a full communications packet to all impacted schools with template outreach emails you can use for your communications, a set of talking points, and a robust FAQ to guide your next steps. But you can also expect questions from parents, teachers and your community who learn about the data breach through the media or other sources.

Do we have to provide notice to our school community and employees about this breach?

If you use PowerSchool and you learn that community data was accessed as part of this incident, your obligations will vary depending on your state law's definition of a reportable incident. In some states, some of the data types exposed do not meet the definition of a "data breach" and thus do not require you to provide any type of notification. Other states may have stricter rules which could require you to provide notice. All states require some form of notification if SSNs were accessed by cybercriminals. If you are unsure about your state obligations, check with your FP attorney or any member of our Privacy and Cyber team.

Even if we have no obligation to do so, should we provide notice to our school community?

Some schools are choosing to provide immediate notice to their community given the prominence in media headlines and the dangers of misinformation filling the void. Moreover, since PowerSchool may contact your teachers and parents directly, it might be in your school's best interest to reach out to your community first to prepare them for such a communication.

What should we communicate to our community?

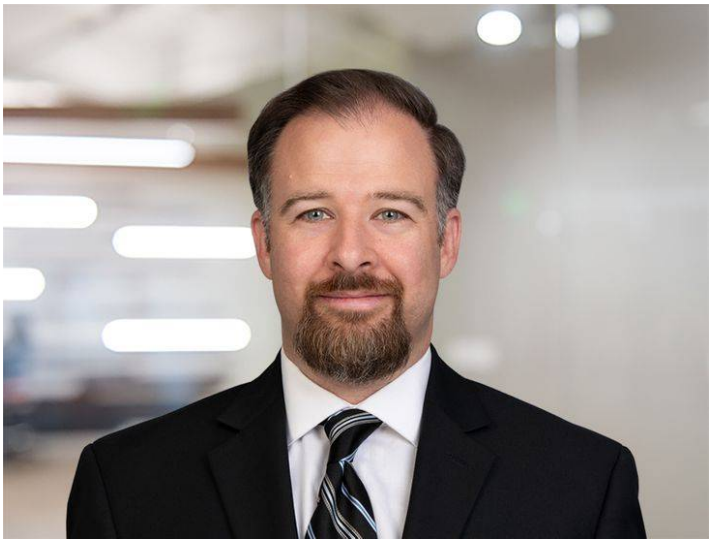
When communicating with your school community about the PowerSchool breach, clarity and transparency are essential. Your message should acknowledge the incident, reassure stakeholders that you are taking appropriate steps to protect their information, let them know that you expect more information from PowerSchool soon, and provide practical guidance. You can reach out to your FP attorney for a sample template you can adapt.

Conclusion

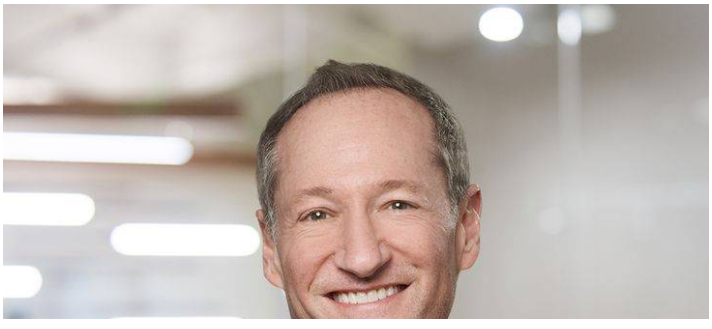
Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have questions, please contact your Fisher Phillips attorney, the author of this Insight, any member of our Education Team, or any member of our Privacy and Cyber Team. You can also rely on our Data Protection and Cybersecurity Team for guidance and support through any such incident.

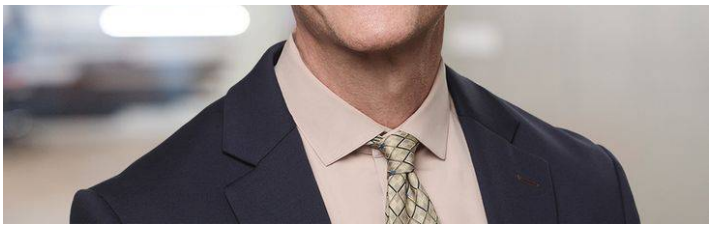
Related People

Jennifer B. Carroll
Partner
954.847.4716
Email



Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate
858.964.1582
Email





Daniel Pepper, CIPP/US
Partner
303.218.3661
Email

Kristin L. Smith
Partner
713.292.5621
Email

Service Focus

Data Protection and Cybersecurity

Privacy and Cyber

Industry Focus

Education

Higher Education