Cyber Threat Escalates: PowerSchool Cybercriminal Returns to Extort Individual Schools Months After Massive Data Breach Purportedly Resolved

Insights
5.09.25

When PowerSchool announced in January that it fell victim to a massive data breach at the end of 2024, it assured the thousands of schools and over 50 million students who use the education software that the matter had been resolved and the stolen data had been deleted. But the threat actor responsible for the initial breach has emerged out of the woodwork for round two, this time extorting individual school districts, threatening to release stolen student and teacher data unless another ransom is paid – even though PowerSchool previously paid a ransom to resolve the matter. Here's what schools (and their communities) need to know about this crucial development and what you should do next.

What Initially Happened?

The initial PowerSchool cyberattack incident occurred in December 2024, exposing millions student and teacher records across thousands of private schools and public school districts. The attack targeted PowerSchool's Student Information System (SIS), which stores sensitive data such as names, addresses, Social Security numbers, and disciplinary records.

According to PowerSchool, the cybercriminals were able to gain full access to the SIS data due to a compromised account lacking multi-factor authentication. The software company also said it paid the threat actor a ransom to delete the data and "believes the data has been deleted without any further replication or dissemination." PowerSchool offered two years of free credit monitoring to the affected individuals, the details of which are provided on PowerSchool's website here.

Click here to read more about the December 2024 incident and how schools navigated the initial fallout.

What Now?

Despite PowerSchool's payment of the ransom, it appears the stolen data was never deleted. The cybercriminals involved in the December 2024 PowerSchool incident are now apparently extorting individual school districts.

PowerSchool has confirmed that the cybercriminal has contacted multiple districts, using data stolen in the original breach. PowerSchool maintains that this is not a new incident, as the leaked data samples are identical to those stolen in the December attack. PowerSchool has reported the extortion attempts to law enforcement in the US and Canada and is working with affected schools. PowerSchool is also encouraging affected individuals to take advantage of the free services they are providing.

Districts have started to release statements which read similarly. For example, a Canadian district released a statement to parents, guardians, and caregivers that the district was made aware that the data was not deleted as previously believed. The announcement also stated that the district is aware that other North American school boards received communication from a threat actor demanding a ransom.

What's Next and What Should You Do?

PowerSchool and law enforcement may share additional details as new information emerges. If you've previously informed your community about this incident, you may want to consider providing an update. However, the extent of potential district impact remains uncertain at this time. As the information involved in the re-extortion seems to be the same information that was impacted in December, it's unlikely that additional notifications will be necessary; however, the analysis will be fact-specific.

Schools that are considering whether to inform their community of this new risk may also want to consult with legal counsel regarding the potential for continued indemnification, as well as the precise drafting of those communications. As with the initial incident, 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.

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 authors of this Insight, any member of our Education Team, or any member of our Data Protection and Cybersecurity Team for guidance and support.

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

Jillian Seifrit, CIPP/US
Associate
610.230.6129
Email

Kristin L. Smith
Partner
713.292.5621
Email

Service Focus

Data Protection and Cybersecurity

Privacy and Cyber

Counseling and Advice

Industry Focus

Education