THOMPSON HINE

Privacy & Cybersecurity Update

January 2025

The PowerSchool Cyber Attack, FERPA, and Data Breach Reporting Compliance

In recent days, several educational institutions have been alerted of a cybersecurity incident impacting PowerSchool, which is a large provider of cloud-based education software in North America. Although information about the incident is still being discovered, educational institutions must activate their data security incident response plans and assess their legal and compliance obligations. Below are frequently asked questions and answers related to this issue, including compliance obligations under the Family Educational Rights and Privacy Act (FERPA) and U.S. state law.

What do we know so far?

According to many media outlets, PowerSchool recently discovered that an unauthorized third party gained access to customer data retained in its PowerSchool Student Information System (SIS). This incident appears to have been contained, and PowerSchool indicated that it is not experiencing any current operational disruptions because of it.

Was this a ransomware attack on PowerSchool?

Based on open-source information, this cybersecurity incident does not appear to be a ransomware attack. Apparently, a third party leveraged compromised credentials to access the PowerSchool SIS.

What type of data has been compromised?

Initial reporting indicates that an unauthorized third party exfiltrated from PowerSchool's information technology (IT) environment certain "tables" related to students and teachers, such as names, telephone numbers, and/or email addresses. For a subset of PowerSchool customers, the compromised data may include more sensitive information, such as health-related details and Social Security numbers (SSN) of current and former students. However, we are awaiting confirmation of the scope of this cybersecurity incident from PowerSchool via a public statement.

What should educational institutions know about their data breach obligations?

There are both federal and state laws governing data breach response. According to the U.S. Department of Education, it "does not have the authority under FERPA to require that agencies or institutions issue a direct notice to a parent or student upon an unauthorized disclosure of education records." However, FERPA does require "that the agency or institution record the disclosure so that a parent or student will become aware of the disclosure during an inspection of the student's education record." In addition, each U.S. state has enacted its own data breach reporting laws, which generally require organizations (including educational institutions) to directly notify individuals when their sensitive personal data has been compromised in a cybersecurity incident.

What are my data breach recordkeeping obligations under FERPA?

Under 34 CFR §99.32(a)(1), educational agencies or institutions are required to maintain a record of each request for and disclosure of personally identifiable information from a student's education records, subject to

specific exceptions and exemptions (see below). This record must be kept alongside the student's education records for as long as those records are maintained. Additionally, the agency or institution must provide a copy of the record upon request by a parent or eligible student.

What is personally identifiable information?

FERPA defines personally identifiable information as including (but not limited to) the following categories of data: (i) the student's name; (ii) the name of the student's parent or other family members; (iii) the address of the student or student's family; (iv) a personal identifier, such as the student's Social Security number, student number, or biometric record; (v) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, (vi) other information that, alone or in combination, is linked or linkable to a specific student who would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (vii) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

What about Directory Information?

FERPA's recordkeeping requirements set forth in §34 CFR 99.32(a)(1) do not apply to, among other areas, the disclosure to a party seeking "directory information." FERPA defines "directory information" as "information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed." The FERPA regulations further provide that "[d]irectory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended." The term "directory information" does not, however, include a student's Social Security number, or certain types of student identification (ID) numbers.

Does the PowerSchool cybersecurity incident implicate U.S. state data breach notifications laws?

It depends. All 50 U.S. states have enacted their own data breach notification laws that require covered organizations to notify individuals when their personal data is compromised in a data breach. The term "personal data" is most often defined to mean unencrypted sensitive personal data, such as a person's Social Security number, driver's license number, and financial account access data. Many states also define personal data to include health and medical information, biometric data, passport identification numbers, state-issued identification numbers, health insurance policy numbers, and account usernames and passwords. There are even some states that define personal data to include an individual's name in conjunction with their date of birth. It is important for each educational institution impacted by the PowerSchool cyber incident to evaluate the types of personal data compromised to assess their notification obligations under U.S. state data breach notification laws.

What are the data breach notification timelines?

Each U.S. state has established its own timelines for when an organization needs to furnish individuals with notice of a data breach. These timeframes range from "as soon as reasonably practicable" to 30 or 60 days, although these timelines are often most stringent/truncated when the incident impacts public schools or other state agencies.

Do we have to inform law enforcement or regulatory authorities?

Many U.S. state laws mandate that state agencies report data breaches impacting residents' personal information to state law enforcement and regulatory agencies. The timelines for reporting such data breaches to regulatory agencies also vary by state law. See the Thompson Hine data breach notification map for more information on data breach reporting obligations under U.S. state law.

Can PowerSchool provide data breach notifications on our behalf?

Pursuant to most U.S. state data breach notifications, a data "controller" (i.e., the educational institution) and not the data "processor" (i.e., PowerSchool) is legally required to comply with the legal obligations to notify affected individuals and regulatory authorities of a data breach. However, it is common practice for the controller and processor to allocate data breach notification responsibilities. In these circumstances, it is important for each party to understand its notification roles and responsibilities to ensure these notifications comply with all aspects of the breach notification law.

Do we have to provide credit monitoring services?

Only a few data breach notification laws require organizations to furnish credit monitoring services in response to a data breach. Further, these laws often require a specific type of personal data, such as a Social Security number, to have been impacted to trigger credit monitoring services to address the heightened risk of identity theft.

Am I at risk of a class action lawsuit?

There have already been lawsuits filed against PowerSchool as a result of this cybersecurity incident. In the last several years, there has been a significant increase in the number of class action lawsuits against organizations on the basis they have been harmed, or will immediately face harm, as a result of the compromise to the confidentiality of their personal data. These claims often center around negligence, negligence *per se*, breach of contract, unjust enrichment, and intrusion upon seclusion. The fact that several regulatory authorities publish the identity of victims of a data breach creates an environment in which they can be more easily targeted for a lawsuit. It is important for educational institutions to identify whether their service contracts require PowerSchool to indemnify them for data breach-related costs, such as third-party claims.

Does my cyber insurance policy cover expenses for responding to the PowerSchool incident?

Each educational institution must assess the nature and scope of its cyber insurance policy to determine which costs they incur from this incident are recoverable. It is common for cyber insurance policies to cover a broad range of cyber incidents, such as ransomware attacks, business email compromise, and unauthorized access to company data, especially personal data. These policies often address circumstances wherein the compromise impacts company data in the custody and control of their third-party service providers. If an educational institution is notified by PowerSchool of this cyber incident, it should consider immediately engaging with its insurance carrier to discuss policy coverage, deductibles, and reservations.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Julie K. Valdes
513.352.6659
Julie.Valdes@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight, Ph.D.
212.908.3971
Thora.Knight@ThompsonHine.com