

Memorandum
PRIVILEGED AND CONFIDENTIAL
ATTORNEY-WORK PRODUCT

To: Scott Gross, Business Administrator
New Boston Central School

From: Meghan Collins, Esq.
Christa Kumming, Esq.
McDonald Hopkins PLC

Date: April 15, 2025

Re: New Boston Central School: Legal Analysis and Risk Assessment of PowerSchool Data
Security Incident

BACKGROUND INFORMATION

New Boston Central School engaged McDonald Hopkins PLC to assist in the legal analysis of and response to a recent data security incident concerning PowerSchool, a company that provides New Boston Central School with student information management software.

On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration of certain personal information from PowerSchool Student Information System (SIS) environments through one of PowerSchool's community-focused customer support portals, PowerSource. According to PowerSchool, the unauthorized actor utilized compromised credentials to access and exfiltrate data from select PowerSchool SIS instances of Students and Teachers tables.

On or about January 7, 2025, PowerSchool informed institutions that certain data within the PowerSchool environment was accessed. The email states, in pertinent part:

... PowerSchool will be providing credit monitoring to affected adults and identity protection services to affected minors in accordance with regulatory and contractual obligations. The particular information compromised will vary by impacted customer. We anticipate that only a subset of impacted customers will have notification obligations.

Exhibit A. On January 27, 2025, PowerSchool commenced email notification to current and former students (or their parents/guardians as applicable) and educators that PowerSchool information was determined to be impacted.

Exhibit B.

PowerSchool submitted notice to Attorneys General on behalf of impacted cloud-hosted institutions on or about January 27, 2025, supplemented on an unspecified date thereafter for on-premise institutions. On January 29, 2025, PowerSchool commenced an email notification campaign to impacted individuals and/or the respective parent or guardian. The notification efforts continued until an undisclosed date in March 2025. The aforementioned email notifications contained a two-year offering of identity protection services for all individuals regardless of the data compromised. Unless an institution affirmatively declined inclusion, PowerSchool provided the email notification to individuals PowerSchool deemed impacted. See **Exhibit B.**

On January 30, 2025, cloud-hosted and on-premise institutions received a plug-in tool from PowerSchool “to query and summarize live PowerSchool SIS data,” however the tool “may not precisely reflect data that was exfiltrated at the time of the incident.” **Exhibit C**. Thereafter, on-premise PowerSchool institutions were required to opt-in to PowerSchool’s email notification campaign.

Based on PowerSchool’s representations and communications about the incident, New Boston Central School understands that the impacted information related to New Boston Central School’s community may have contained personal information of certain individuals, including one or more of the following: name, date of birth, and/or limited medical alert information. According to PowerSchool, no other personal information belonging to New Boston Central School was impacted by the data security incident.

On March 7, 2025, PowerSchool published a report summarizing its forensic firm’s investigation findings. **See Exhibit D**.

The purpose of this memorandum is to determine New Boston Central School’s notification obligations, if any, under the State of New Hampshire’s data breach notification statute, **N.H. RSA §§ 359-C:19 *et seq.*** or the Family Educational Rights and Privacy Act of 1974 (“FERPA”), **20 U.S.C. § 1232g; 34 CFR Part 99**.

LEGAL ANALYSIS – STATE LAW

This incident was analyzed under New Hampshire law for illustrative purposes because New Boston Central School is located in New Hampshire.¹ Notification (to affected individuals, regulators, and media) is required under New Hampshire’s data breach notification statute when there has been a “[s]ecurity breach” impacting “[p]ersonal information”. The facts here do not fit either definition; therefore, notice is not required under the statute.²

Pursuant to N.H. RSA § 359-C:19(V), “[s]ecurity breach” is defined as:

[The] unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person’s business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Pursuant to N.H. RSA § 359-C:19(IV), “[p]ersonal information” is defined as:

- a. [A]n individual’s first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
 - 1) Social security number.
 - 2) Driver’s license number or other government identification number.
 - 3) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
- b. “Personal information” shall not include information that is lawfully made available to the general public from federal, state, or local government records.

Based on the facts set forth above, this incident does not meet the threshold definitions.

¹ Notification obligations are determined by the states of residence of the individuals whose information was potentially exposed and not where an entity is located. Nevertheless, none of the states’ breach notice laws are triggered by this incident.

² Under the respective state data breach notification definitions, date of birth only constitutes personal information in Washington and North Dakota. Similarly, student identification number is only considered personal information in Washington and Colorado. See Colo. Rev. Stat. § 6-1-716(1)(g); N.D. Cent. Code § 51-30-01(4); Wash. Rev. Stat. § 19.255.005(2).

As noted above, PowerSchool did identify potentially sensitive or personally identifiable information attributable to New Boston Central School data impacted by this incident. However, the information identified only included date of birth and medical alert information, neither of which is considered “[p]ersonal information” for residents of New Hampshire. Thus, because this incident did not involve the “unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information”, New Hampshire’s data breach notice law is not triggered and there are no notification obligations arising out of this incident.

LEGAL ANALYSIS UNDER FERPA

The Family Educational Rights and Privacy Act of 1974 (“FERPA”) is the federal statute covering student records. See 34 CFR § 99. FERPA does not have an express breach notification requirement for unauthorized disclosures. FERPA does, however, require the institution to record unauthorized disclosure of non-directory information in a student’s education record. Direct student notification is advisable if the compromised data includes student Social Security numbers and other identifying information that could lead to identity theft.³ Disclosure of non-directory information contained in a student’s education record requires authorization from the student and/or parent.

Pursuant to Section 99.3, “disclosure” is defined as:

Disclosure means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record.

Pursuant to Section 99.3, “education record” is defined as:

- (a) The term means those records that are:
 - (1) Directly related to a student; and
 - (2) Maintained by an educational agency or institution or by a party acting for the agency or institution.
- (b) The term does not include:
 - (1) Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.
 - (2) Records of the law enforcement unit of an educational agency or institution, subject to the provisions of § 99.8.
 - (3) (i) Records relating to an individual who is employed by an educational agency or institution, that: (A) Are made and maintained in the normal course of business; (B) Relate exclusively to the individual in that individual’s capacity as an employee; and (C) Are not available for use for any other purpose; (ii) Records relating to an individual in attendance at the agency or institution who is employed as a result of his or her status as a student are education records and not excepted under paragraph (b)(3)(i) of this definition. 34 CFR § 99.3.

With respect to directory information, FERPA does not bar disclosure by the educational institution. Section 99.3 defines “directory information” as:

- (a) *Directory information* includes, but is not limited to, the student’s name; address; telephone listing (including mobile phone number); 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

³ Family Educational Rights and Privacy, Final Rule, 73 Federal Register 74843-74844 [December 9, 2008].

of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended.

(b) Directory information does not include a student's –

- (1) Social security number; or
- (2) Student identification (ID) number, except as provided in paragraph (c) of this definition.

(c) In accordance with paragraphs (a) and (b) of this definition, directory information includes –

- (1) A student ID number, user ID, or other unique personal identifier used by a student for purposes of accessing or communicating in electronic systems, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a personal identification number (PIN), password or other factor known or possessed only by the authorized user; and
- (2) A student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user. *Id.*

Section 99.32 addresses what recordkeeping requirements exist concerning requests and disclosures. It states in pertinent part: An educational agency or institution must maintain a record of each request for access to and each disclosure of personally identifiable information from the education records of each student, as well as the names of State and local educational authorities and Federal officials and agencies listed in Section 99.31(a)(3) that may make further disclosures of personally identifiable information from the student's education records without consent under Section 99.33(b).⁴

In this instance, based on PowerSchool's inability and/or refusal to provide detailed information about the information potentially impacted that may be considered directory information, New Boston Central School is placing a FERPA recordation in each identifiable persons educational record out of an abundance of caution.

CONCLUSION

Based on the facts set forth above, PowerSchool's representations and forensic investigation findings, and the legal analysis conducted herein, New Boston Central School is not required to notify any individuals, the media, or federal/state regulators of this incident, despite PowerSchool's email notification campaign. Further, New Boston Central School is placing a recordation of the incident in all identifiable student education records out of an abundance of caution. McDonald Hopkins' legal assessment is based on the facts and information known at the time and reserves the right to revise its assessment should new information become available.

Records of this incident should be maintained for five (5) years.

⁴ 34 CFR Part 99.32(a)(1).

Exhibit A

Dear Valued Customer,

As the Technical Contact for your district or school, we are reaching out to inform you that on December 28, 2024, PowerSchool became aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed.

Please review the following information and be sure to share this with relevant security individuals at your organization.

As soon as we learned of the potential incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We have also informed law enforcement.

We can confirm that the information accessed belongs to certain SIS customers and relates to families and educators, including those from your organization. The unauthorized access point was isolated to our PowerSource portal. As the PowerSource portal only permits access to the SIS database, **we can confirm no other PowerSchool products were affected as a result of this incident.**

Importantly, the incident is contained, and we have no evidence of malware or continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor expects to experience, any operational disruption and continues to provide services as normal to our customers.

Rest assured, we have taken all appropriate steps to prevent the data involved from further unauthorized access or misuse. We do not anticipate the data being shared or made public, and we believe it has been deleted without any further replication or dissemination.

We have also deactivated the compromised credential and restricted all access to the affected portal. Lastly, we have conducted a full password reset and further tightened password and access control for all PowerSource customer support portal accounts.

PowerSchool is committed to working diligently with customers to communicate with your educators, families, and other stakeholders. We are equipped to conduct a thorough notification process to all impacted individuals. Over the coming weeks, we ask for your patience and collaboration as we work through the details of this notification process.

We have taken all appropriate steps to further prevent the exposure of information affected by this incident. While we are unaware of and do not expect any actual or attempted misuse of personal information or any financial harm to impacted individuals as a result of this incident, PowerSchool will be providing credit monitoring to affected adults and identity protection services to affected minors in accordance with regulatory and contractual obligations. The particular information compromised will vary by impacted customer. We anticipate that only a subset of impacted customers will have notification obligations.

In the coming days, we will provide you with a communications package to support you in engaging with families, teachers and other stakeholders about this incident. The communications package will include tailored outreach emails, talking points, and a robust FAQ so that district and school leadership can confidently discuss this incident with your community.

We understand that you may have additional questions as a result of this update. FAQs are available on [PowerSchool Community](#). Additionally, we will be holding webinars with senior leaders, including our Chief Information Security Officer, to address additional concerns. Please click the link below to register for a webinar that fits your schedule. Note that content for all sessions will be identical, so you need only attend one.

Wednesday, January 8: [REGISTER HERE](#)

Thursday, January 9: [REGISTER HERE](#)

In the meantime, please reach out to your Customer Success Manager (CSM), Support, or other established PowerSchool contact should you have any questions. We will be sending communications later today to other stakeholders in your organization who are responsible for other PowerSchool products notifying them of no impact to the other PowerSchool products.

We are addressing the situation in an organized and thorough manner, and we are committed to providing affected customers with the resources and support they may need as we work through this together.

Thank you for your continued support and partnership.

Sincerely,
Hardeep Gulati
[Chief Executive Officer](#)

Paul Brook
[Chief Customer Officer](#)

cc: **Mishka McCowan**
[Chief Information Security Officer](#)



[PowerSchool](#) •

Copyright © , PowerSchool Group LLC. All rights reserved. [Unsubscribe](#)

Exhibit B

PowerSchool Cybersecurity Incident

This site will be updated periodically as PowerSchool learns more information and takes additional steps in response to a recent security incident.

March 7, 2025

Summary Update

To our customers and the communities we serve, we would like to extend our gratitude and deepest appreciation for your patience and understanding as we have worked diligently to navigate the cybersecurity incident. We would like to provide a final update on this incident, though this website and the resources mentioned will continue to be available in the coming months.

What Happened?

On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration of personal information from certain PowerSchool Student Information System (SIS) environments through one of our community-focused customer support portals, PowerSource. PowerSchool did not experience any operational disruption and continued to provide services as normal to our customers.

Steps We're Taking in Response

As soon as we learned of the incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. **We have no evidence that other PowerSchool products were affected as a result of this incident, or that there is any malware or continued unauthorized activity in the PowerSchool environment.** Districts and schools that do not utilize PowerSchool SIS were not affected.

What Information Was Involved?

Information related to current and former students and educators involved included one or more of the following, which varied by person: name, contact information, date of birth, limited medical alert information, Social Security Number (SSN)/Social Insurance Number (SIN), and other related information. We have no evidence that credit card or banking information was involved. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base.

Notification to Individuals, Credit Monitoring, & Identity Protection

PowerSchool has notified relevant regulators on our customers' behalf in applicable jurisdictions as well as students (or their parents/guardians) and educators in the U.S. and Canada. In these geographies, we have offered complimentary identity protection services including, if applicable, credit monitoring services, for involved students and educators, regardless of whether an individual's Social Security Number/Social Insurance Number was exfiltrated. In countries outside of the U.S. and Canada where the provider provides such services, PowerSchool is offering two years of complimentary identity protection services for all students and educators whose information was involved, regardless of what information about an individual was exfiltrated.

CrowdStrike Incident Report

PowerSchool engaged CrowdStrike, an industry leading cybersecurity expert, as soon as we became aware of the incident. After a thorough investigation, CrowdStrike has submitted its final incident report which you can read [here](#).

CrowdStrike did not identify any new or concerning findings beyond what we already shared; these findings include:

- 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.

Our Commitment Moving Forward

PowerSchool is committed to protecting the security and integrity of our applications and regularly reviews and enhances its security policies and practices, and we will continue to prioritize and invest significantly in our cybersecurity defenses. PowerSchool takes our responsibility to protect student, family and educator data privacy extremely seriously, and we are committed to taking further steps to strengthen the security of our systems.

FAQs

Who is PowerSchool?

PowerSchool provides cloud-based software to K-12 schools. This security incident affected some of the districts using the PowerSchool Student Information System product. We have no evidence that any other PowerSchool products were affected as a result of this incident.

Who is eligible for complimentary identity protection services and credit monitoring?

PowerSchool is offering complimentary identity protection services including, if applicable, credit monitoring services, for involved students and educators, regardless of whether an individual's Social Security Number/Social Insurance Number was exfiltrated. In countries outside of the U.S. and Canada where the provider provides such services, PowerSchool is offering two years of complimentary identity protection services for all students and educators whose information was involved, regardless of what information about an individual was exfiltrated.

How do I sign up for identity protection services and credit monitoring services?

For individuals who reside in the U.S., you can find more information on identity protection services and credit monitoring here: <https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>

For individuals who reside in the Canada, you can find more information on identity protection services and credit monitoring here: <https://www.powerschool.com/security/sis-incident/notice-of-canada-data-breach/>

For individuals who reside outside the U.S. and Canada in a country where the provider provides identity protection services, your school or district will have access to information about such services.

If my information was involved, how will I be notified?

PowerSchool is coordinating with Experian and TransUnion to provide notice on behalf of our customers (in the U.S. and Canada) to students (or their parents / guardians) and educators, as applicable, whose information was involved and for whom we had available contact information. If you reside outside of the U.S. and Canada, you may be notified by your school or district directly.

What if I don't get an email?

If you reside in the U.S. and do not receive an email, you can find more information linked here:

<http://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>

If you reside in Canada and do not receive an email, you can find more information linked here:

<https://www.powerschool.com/security/sis-incident/notice-of-canada-data-breach/>

Would PowerSchool reach out to me directly to request my personal information?

No, PowerSchool will never contact you by phone or email to request your personal or account information. You may receive an email from Experian on behalf of PowerSchool, which will provide information about enrolling in Experian or TransUnion services, as applicable.

Were other PowerSchool products affected?

We have no evidence that other PowerSchool products were affected as a result of this incident. Districts and schools that do not utilize PowerSchool SIS were not affected.

Why does the data involved vary by customer?

This is because the information stored in a customer's SIS is dependent on customer choice or district policies and requirements.

Do we need to secure our own systems as a result of PowerSchool's cybersecurity incident?

We do not believe there is an ongoing risk to our systems. We have no evidence of malware or continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers.

Has PowerSchool distributed a press release related to this incident?

Yes. In accordance with applicable laws and regulations, PowerSchool has distributed a press release via Business Wire in the [United States](#) and [Canada](#) an effort to inform the majority of those whose information was involved as a result of the incident.

Notices of Data Breach

 [Notice of Data Breach For Individuals in the United States](#)

General Updates

January 27, 2025: PowerSchool Notifies Applicable Attorneys General Offices Regarding Cybersecurity Incident —

PowerSchool Notifies Applicable Attorneys General Offices Regarding Cybersecurity Incident

As we have communicated previously, on December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration of personal information from certain PowerSchool Student Information System (SIS) environments. Related to that incident, today, January 27, 2025, PowerSchool began the process of filing regulatory notifications with Attorneys General Offices across applicable U.S. jurisdictions on behalf of impacted customers who have not opted-out of our offer to do so. PowerSchool has also started the process of notifying Canadian regulators. We will provide a separate update to our international customers later this week.

Some U.S. customers may also have notification requirements with their state's Department of Education where required. Since many customers have already notified and are in close contact with their state's Department of Education, PowerSchool will defer to those customers on making these notifications.

We are providing this update for broad awareness, and no further action is required from our customers at this time. In the coming days, PowerSchool will begin to provide notification of the cybersecurity incident to current and former students (or their parents / guardians as applicable) and educators whose information was determined to be involved. **Importantly, these notices will include instructions for involved individuals on how to enroll in the credit monitoring and identity protection services that are being offered by PowerSchool.**

We will be in contact directly with customers again soon with more information. Thank you to our customers, and their broader communities, for their ongoing patience and partnership.

Status Update

Thank you for your continued patience as we navigate this cybersecurity incident. As we reported last week, PowerSchool will be offering complimentary identity protection services as applicable for all students and educators whose information was involved, plus two years of credit monitoring for adults, regardless of whether an individual's Social Security Number or Social Insurance Number was exfiltrated. As we move forward with the process of notifying students and educators whose information was involved, as well as regulators on our customer's behalf, we will provide another update in the next few days.

In addition to regularly updating the various FAQs on this web page, we want to address a recurring question: what data was involved, and for how many schools and individuals? We cannot confirm precise numbers because our data review process is still ongoing. Further, it is difficult to make broad statements about what data was involved because the answer varies by individual customer and is dependent on customer choice or district policies and requirements. We continue to prioritize transparent and direct communication with our customers and our shared communities, and remain committed to providing accurate and transparent updates as more information becomes available. We want to again extend our gratitude to our customers and the students, families and educators we serve. We are dedicated to using this incident as an opportunity to grow stronger and build greater resilience as a company.

What Happened

On December 28, 2024, we became aware of a potential cybersecurity incident involving unauthorized access to certain PowerSchool Student Information System (SIS) information through one of our community-focused customer portals, PowerSource.

PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers. We have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.

Steps We're Taking in Response

As soon as we learned of the incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We are working to complete our investigation of the incident and are coordinating with districts and schools to provide more information and resources (including credit monitoring or identity protection services if applicable) as they become available.

Who Was Affected

On January 7, 2025, we proactively communicated this incident to the PowerSchool SIS customers affected by this incident, and we continue to support them through next steps. Districts and schools that do not utilize PowerSchool SIS were not affected. If you are a parent or guardian who wants to know if your school was involved, please reach out to your school directly.

Moving Forward

We take our responsibility to protect student, family, and educator data privacy extremely seriously, and we are committed to providing customers, families, and educators with resources and support as we work through this together.

We would like to extend a sincere note of gratitude to our customer, educator and family communities for their continued patience and cooperation. We apologize for any concern this incident may cause you and are working hard to provide you timely updates.

General FAQ

What happened?

On December 28, 2024, we became aware of a potential cybersecurity incident involving unauthorized access to certain PowerSchool SIS information through one of our community-focused customer portals, PowerSource. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers. We have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.

When will PowerSchool provide next steps to schools, educators and families?

We are working to complete our investigation of the incident and are coordinating with districts and schools to provide more information and resources (including credit monitoring or identity protection services if applicable) as they become available.

What steps are you taking to prevent this from happening again?

PowerSchool is committed to protecting the security and integrity of our applications and regularly reviews and enhances its security policies and practices. We continue to prioritize and invest significantly in our cybersecurity defenses.

What is the timeline for providing notification information to schools, educators and families?

As PowerSchool is working to complete our investigation, we are also taking steps to set up a system – in coordination with our customers – to be able to provide supportive resources (including credit monitoring or identity protection services if applicable) for individuals whose data may have been involved. As we have more definitive information on our timeline, we will share that accordingly.

FAQ for Families

Who is PowerSchool?

PowerSchool provides cloud-based software to K-12 schools. This security incident affected some of the districts using the PowerSchool Student Information System product. We have no evidence that any other PowerSchool products were affected as a result of this incident.

Am I required to reach out to my school or take any steps as a parent or guardian at this time?

No. If you are a parent or guardian of a student under the age of 18 and your student's information was exfiltrated from their district's PowerSchool SIS, you may receive a notification email from PowerSchool. Additionally, we have posted on our website and distributed a media release informing individuals of the incident and resources we have offered.

Was any student or family data involved in this incident?

For involved current and former students, parents / guardians of students, and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Security Number (SSN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base. The majority of individuals did not have their medical alert information or Social Security Number involved.

Was credit card or banking information involved in this incident?

We have no evidence that credit card or banking information was involved.

Is PowerSchool offering credit monitoring?

We are working to complete our investigation of the incident and are coordinating with districts and schools to provide more information and resources (including credit monitoring or identity protection services if applicable) as they become available.

Would PowerSchool reach out to me directly to discuss this incident, including requesting my personal information?

PowerSchool is committed to keeping our community informed and will be providing further resources as they become available. However, please remain vigilant as PowerSchool will never contact you by phone or email to request your personal or account information.

FAQ for Educators

Was any educator data involved in this incident?

Across our customer base, we have determined that for a portion of individuals, some personally identifiable information (PII), such as social security numbers (SSN) and medical information, was involved. We are working with urgency to

complete our investigation and identify the individuals whose data may have been involved.

Was credit card or banking information involved in this incident?

We have no evidence that credit card or banking information was involved.

Is PowerSchool offering credit monitoring?

We are working to complete our investigation of the incident and are coordinating with districts and schools to provide more information and resources (including credit monitoring or identity protection services if applicable) as they become available.

How many districts and schools were involved?

Because of our ongoing investigation, we are not sharing specifics around the number of districts and schools we believe were involved. We are in communication with those customers directly and are supporting them through next steps.

FAQ for Customers

Was data from my school district involved?

We have proactively contacted the SIS customers that we believe may have had data involved. If you are not a SIS customer, you were not affected.

Should we take any action to secure our own systems?

We do not believe there is an ongoing risk to our systems. We have no evidence of malware or continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers.

Were other PowerSchool products affected?

Other than PowerSchool SIS, we have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.

U.S. Updates

Identity and Credit Monitoring Update for United States Customers

Since our last update, we have initiated the process of notifying involved individuals in the U.S. about the resources now available to them. As part of this process, we have posted a notice to our website and published a press release. Credit monitoring and identity protection services are now activated and available.

In the coming weeks, Experian (on behalf of PowerSchool) will also be distributing direct email notifications to involved individuals for whom we have sufficient contact information. This does not apply to customers who have opted out of this process. The email notice will include further information about the information of theirs involved and the resources PowerSchool is offering. Additionally, we have coordinated with Experian to set up a toll-free call center for families and educators in case they have questions about these offerings: [833-918-9464](tel:833-918-9464)

For individuals located in Canada, we will be reaching out next week with further information on the resources made available to you.

To our customers and the families and educators that we serve, please know that we sincerely appreciate your continued patience throughout this process. We remain committed to supporting you.

General FAQ

What is the timeline for providing notification information to schools, educators and families?

PowerSchool initiated notifying our customers on January 7, as well as individuals on January 29 by posting a notice to our website, and publishing a press release. In the coming weeks, direct email notifications will go out to involved students and educators for whom we have sufficient contact information.

FAQ for Families

Why is Experian notifying me instead of PowerSchool?

PowerSchool has engaged Experian, a trusted credit reporting agency, to provide complimentary identity protection and credit monitoring services on behalf of PowerSchool and our customers who opted in to these services. Additionally,

PowerSchool worked with Experian to set up a dedicated, toll-free call center to answer any questions regarding the incident that involved individuals may have.

How do I sign up for credit monitoring?

For details on how to sign up for the resources being offered and how to reach the dedicated call center, you will be receiving an e-mail notification directly from PowerSchool in the coming days, or you can visit their website to learn how to activate the offerings from Experian, linked

here: <https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>

What if I don't get an email?

Involved individuals may receive an email communication in the coming weeks. If you do not receive an email, you can find more information linked

here: <https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/> This notification provides details about the support resources we are offering, including complimentary credit monitoring and identity protection services if you do not receive a direct email.

What information of mine was involved?

For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Security Number (SSN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base. Please note regardless of whether an individual's Social Security Number was exfiltrated, we are offering **two years of complimentary identity protection services** for all current and former students, parents / guardians of students, and educators whose information was determined to be involved. We are also offering **two years of complimentary credit monitoring services** for all adult students, and educators whose information was determined to be involved.

FAQ for Educators

Why is Experian notifying me instead of PowerSchool?

PowerSchool has engaged Experian, a trusted credit reporting agency, to provide complimentary identity protection and credit monitoring services on behalf of PowerSchool and our customers who opted in to these services. Additionally, PowerSchool worked with Experian to set up a dedicated, toll-free call center to answer any questions regarding the incident that involved individuals may have.

How do I sign up for credit monitoring?

For details on how to sign up for the resources being offered and how to reach the dedicated call center, you will be receiving an e-mail notification directly from PowerSchool in the coming days, or you can visit their website to learn how to activate the offerings from Experian, linked here: <https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>.

What if I don't get an email?

Involved individuals may receive an email communication in the coming weeks. If you do not receive an email, you can find more information linked here: <https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>. This notification provides details about the support resources we are offering, including complimentary credit monitoring and identity protection services if you do not receive a direct email.

FAQ for Customers

How will students and educators be notified if their information was involved?

We have initiated the process of notifying involved individuals. In the coming weeks following Jan. 29, direct email notifications will go out, and in the meantime, we have distributed a media release and posted a notice to our website.

Updated Information for U.S. Families, Educators and Customers

What Happened

On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration of personal information from certain PowerSchool Student Information System (SIS) environments through one of our community-focused customer support portals, PowerSource. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers. We have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.

Identity Protection & Credit Monitoring Services

PowerSchool will be offering two years of complimentary identity protection services for all students and educators whose information was involved and will also be offering two years of complimentary credit monitoring services for all adult students and educators whose information was involved. We are doing this regardless of whether an individual's Social Security Number was exfiltrated. PowerSchool has engaged Experian, a trusted credit reporting agency, to provide these services. Starting in the next few weeks, PowerSchool will coordinate with Experian to provide notice on behalf of our customers to students (or their parents/guardians if the student is under 18) and educators whose information was exfiltrated from their PowerSchool SIS.

Student and Educator Data Involved

For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Security Number (SSN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base.

Who Was Affected

On January 7, 2025, we proactively communicated this incident to the PowerSchool SIS customers affected by this incident. On January 17, 2025, PowerSchool shared next steps with those same SIS customers. Districts and schools that do not utilize PowerSchool SIS were not affected.

Steps We Are Taking in Response & Moving Forward

As soon as we learned of the incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. Since then, over the last few weeks, we have been focused on assessing the scope of data involved, making further enhancements to our cybersecurity defenses, and developing a plan to help you and our shared community. We take our responsibility to protect student, family, and educator data privacy extremely seriously, and we are committed to providing customers, families, and educators with resources and support as we work through this together.

General FAQ

What happened?

On December 28, 2024, we became aware of a potential cybersecurity incident involving unauthorized access to certain PowerSchool SIS information through one of our community-focused customer portals, PowerSource. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers. We have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.

When will PowerSchool provide next steps to schools, educators and families?

We are working to complete our investigation of the incident and are coordinating with districts and schools to provide more information and resources (including credit monitoring or identity protection services if applicable) as they become available.

What steps are you taking to prevent this from happening again?

PowerSchool is committed to protecting the security and integrity of our applications and regularly reviews and enhances its security policies and practices. We continue to prioritize and invest significantly in our cybersecurity defenses.

What is the timeline for providing notification information to schools, educators and families?

As PowerSchool is working to complete our investigation, we are also taking steps to set up a system – in coordination with our customers – to be able to provide supportive resources (including credit monitoring or identity protection services

if applicable) for individuals whose data may have been involved. As we have more definitive information on our timeline, we will share that accordingly.

FAQ for Families

Who is PowerSchool?

PowerSchool provides cloud-based software to K-12 schools. This security incident affected some of the districts using the PowerSchool Student Information System product. We have no evidence that any other PowerSchool products were affected as a result of this incident.

Am I required to reach out to my school or take any steps as a parent or guardian at this time?

No. If you are a parent or guardian of a student under the age of 18 and your student's information was exfiltrated from their district's PowerSchool SIS, you may receive a notification email from PowerSchool. Additionally, we have posted on our website and distributed a media release informing individuals of the incident and resources we have offered.

Was any student or family data involved in this incident?

For involved current and former students, parents / guardians of students, and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Security Number (SSN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base. The majority of individuals did not have their medical alert information or Social Security Number involved.

Was credit card or banking information involved in this incident?

We have no evidence that credit card or banking information was involved.

Will I get identity protection or credit monitoring?

PowerSchool is offering complimentary identity protection and credit monitoring services to all students and educators whose information from your PowerSchool SIS was involved. This offer is being provided regardless of whether an individual's Social Security number was exfiltrated.

- **Identity Protection:** PowerSchool will be offering two years of complimentary identity protection services, which will be provided by Experian, for all students and educators whose information was involved.
- **Credit Monitoring:** PowerSchool will also be offering two years of complimentary credit monitoring services, which will be provided by TransUnion, for all students and

educators who have reached the age of majority whose information was involved.

Credit monitoring agencies do not offer credit monitoring services for individuals under the age of majority. If a parent / guardian enrolls an individual under the age of majority in the offered identity protection services, the individual, upon reaching the age of majority, will have the opportunity to enroll in credit monitoring services for the duration of the two-year coverage period.

Would PowerSchool reach out to me directly to request my personal information?

PowerSchool is committed to keeping our community informed and will be providing further resources as they become available. However, please remain vigilant as PowerSchool will never contact you by phone or email to request your personal or account information.

Why is Experian notifying me instead of PowerSchool?

PowerSchool has engaged Experian, a trusted credit reporting agency, to provide complimentary identity protection and credit monitoring services on behalf of PowerSchool and our customers who opted in to these services. Additionally, PowerSchool worked with Experian to set up a dedicated, toll-free call center to answer any questions regarding the incident that involved individuals may have.

How do I sign up for credit monitoring?

For details on how to sign up for the resources being offered and how to reach the dedicated call center, you will be receiving an e-mail notification directly from PowerSchool in the coming days, or you can visit their website to learn how to activate the offerings from Experian, linked here:

<http://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>

What if I don't get an email?

Involved individuals may receive an email communication in the coming weeks. If you do not receive an email, you can find more information linked here:

<http://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>.

This notification provides details about the support resources we are offering, including complimentary credit monitoring and identity protection services if you do not receive a direct email.

What information of mine was involved?

For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social

Security Number (SSN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base.

Please note regardless of whether an individual's Social Security Number was exfiltrated, we are offering **two years of complimentary identity protection services** for all current and former students, parents / guardians of students, and educators whose information was determined to be involved. We are also offering **two years of complimentary credit monitoring services** for all adult students, and educators whose information was determined to be involved.

FAQ for Educators

Was any educator data involved in this incident?

For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Insurance Number (SIN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base. The notice received by each individual will include a description of the categories of personal information that were exfiltrated and the identity protection and credit monitoring services offered (as applicable).

Was credit card or banking information involved in this incident?

We have no evidence that credit card or banking information was involved.

Is PowerSchool offering identity protection and credit monitoring services?

PowerSchool will be offering two years of complimentary identity protection services for all students and educators whose information was involved and will also be offering two years of complimentary credit monitoring services for all students who have reached the age of majority and educators whose information was involved. We are doing this regardless of whether an individual's Social Security Number was exfiltrated.

How many districts and schools were involved?

We are not sharing specifics around the number of districts and schools we believe were involved. We are in communication with those customers directly and are supporting them through next steps.

Why is Experian notifying me instead of PowerSchool?

PowerSchool has engaged Experian, a trusted credit reporting agency, to provide complimentary identity protection and credit monitoring services on behalf of PowerSchool and our customers who opted in to these services. Additionally, PowerSchool worked with Experian to set up a dedicated, toll-free call center to answer any questions regarding the incident that involved individuals may have.

How do I sign up for credit monitoring?

For details on how to sign up for the resources being offered and how to reach the dedicated call center, you will be receiving an e-mail notification directly from PowerSchool in the coming days, or you can visit their website to learn how to activate the offerings from Experian, linked here:

<http://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>.

What if I don't get an email?

Involved individuals may receive an email communication in the coming weeks. If you do not receive an email, you can find more information linked here:

<http://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>.

This notification provides details about the support resources we are offering, including complimentary credit monitoring and identity protection services if you do not receive a direct email.

FAQ for Customers

Was data from my school district involved?

We have proactively contacted the SIS customers that we believe were affected. If you are not a SIS customer, you were not affected.

Should we take any action to secure our own systems?

We do not believe there is an ongoing risk to our systems. We have no evidence of malware or continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers.

Were other PowerSchool products affected?

Other than PowerSchool SIS, we have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.

How will students and educators be notified if their information was involved?

We have initiated the process of notifying involved individuals. In the coming weeks following Jan. 29, direct email notifications will go out, and in the meantime, we have distributed a media release and posted a notice to our website.

Canada & International Updates

February 5, 2025: International Customer Update



International Customer Update

PowerSchool has continued the process of notifying customers outside of the United States and Canada whose SIS was determined to be involved in this incident. In countries where Experian offers such services, PowerSchool will be offering two years of complimentary identity protection services for all students and educators whose information was involved, regardless of what information about an individual was exfiltrated. Due to available or applicable offerings in certain countries, we are not able to offer identity protection and/or credit monitoring services to all students and educators outside of the United States and Canada.

Individuals whose information was involved who reside outside of the United States and Canada may be notified by their school or district directly. The types of information involved in this incident included one or more of the following, which varied by person: name, contact information, date of birth, limited medical alert information, and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base.

To our customers and the families and educators that we serve, please know that we sincerely appreciate your continued patience throughout this process. We remain committed to supporting you, and we sincerely regret any concern this incident may have caused.

Identity and Credit Monitoring Update for Canadian Customers

Since our last update, we have initiated the process of notifying involved students and educators in Canada about the resources now available to them. As part of this process, we have posted a notice to our website and published a press release. Credit monitoring and identity protection services are now activated and available for students and educators whose information was determined to be involved.

For individuals located in Canada, we have engaged Experian and TransUnion, trusted credit reporting agencies, to provide complimentary identity protection and credit monitoring services on behalf of PowerSchool to involved students and educators.

In the coming weeks, Experian (on behalf of PowerSchool) will also be distributing direct email notifications to involved students (or the parents / guardians of students, as applicable) and educators for whom we have sufficient contact information. The email notice will include further information about the information of theirs involved and the resources we are offering. Additionally, we have coordinated with Experian to set up a toll-free call center for families and educators in case they have questions about these offerings: 833-918-9464, Monday through Friday, 8:00am through 8:00pm Central Time (excluding major US holidays).

To our customers and the families and educators that we serve, please know that we sincerely appreciate your continued patience throughout this process. We remain committed to supporting you.

General FAQ

What is the timeline for providing notification information to schools, educators and families?

PowerSchool initiated notifying our customers on January 7, as well as individuals on January 29 by posting a notice to our website, and publishing a press release. In the coming weeks, direct email notifications will go out to involved students and educators for whom we have sufficient contact information.

FAQ for Families

When will I be able to access the identity protection or credit monitoring?

All the information regarding the activation of and access to these services will be included in the email sent to you by Experian. You may also visit [our website linked here](#) for information on how to activate these services.

Why is Experian notifying me instead of PowerSchool?

PowerSchool has engaged Experian to provide notification of complimentary identity protection and credit monitoring services (which in Canada are offered by Transunion, a trusted credit reporting agency) on behalf of PowerSchool and our customers. Additionally, PowerSchool worked with Experian to set up a dedicated, toll-free call center to answer any questions regarding the incident and the services provided to involved individuals.

How do I sign up for credit monitoring?

For details on how to sign up for the resources being offered and how to reach the dedicated call center, you will be receiving an e-mail notification directly from Experian in the coming weeks that includes information about how to sign-up for TransUnion. You may also visit [our website linked here](#) to learn how to activate the offerings from Experian and TransUnion.

What if I don't get an email?

Involved students (or parents / guardians of students, as applicable) and educators may receive an email communication in the coming weeks. If you do not receive an email, you can find more information on [our website linked here](#). This notification provides details about the support resources we are offering, including complimentary credit monitoring and identity protection services if you do not receive a direct email.

FAQ for Educators

Why is Experian notifying me instead of PowerSchool?

PowerSchool has engaged Experian to provide notification of complimentary identity protection and credit monitoring services (which in Canada are offered by Transunion, a trusted credit reporting agency) on behalf of PowerSchool and our customers. Additionally, PowerSchool worked with Experian to set up a dedicated, toll-free call center to answer any questions regarding the incident and the services provided to involved individuals.

How do I sign up for credit monitoring?

For details on how to sign up for the resources being offered and how to reach the dedicated call center, you will be receiving an e-mail notification directly from Experian in the coming weeks that includes information about how to sign-up for TransUnion. You may also [visit our website linked here](#) to learn how to activate the offerings from Experian and TransUnion.

What if I don't get an email?

Involved students (or parents / guardians of students, as applicable) and educators may receive an email communication in the coming weeks. If you do not receive an email, you can find more information on our website linked here. This notification provides details about the support resources we are offering, including complimentary credit monitoring and identity protection services if you do not receive a direct email.

FAQ for Customers

How will students and educators be notified if their information was involved?

We have initiated the process of notifying involved individuals. In the weeks following Feb. 3, direct email notifications will go out to students (or parents / guardians of students, as applicable) and educators determined to have information involved, and in the meantime, we have distributed a media release and posted a notice to our website. We continue to work in coordination with our customers to reach individuals involved in this incident.

Updated Information for Canada Families, Educators and Customers

Status Update

Thank you for your continued patience as we navigate this cybersecurity incident. As we reported last week, PowerSchool will be offering complimentary identity protection services as applicable for all students and educators whose information was involved, plus two years of credit monitoring for adults, regardless of whether an individual's Social Security Number or Social Insurance Number was exfiltrated. As we move forward with the process of notifying students and educators whose information was involved, as well as regulators on our customer's behalf, we will provide another update in the next few days.

In addition to regularly updating the various FAQs on this web page, we want to address a recurring question: what data was involved, and for how many schools and individuals? We cannot confirm precise numbers because our data review process is still ongoing. Further, it is difficult to make broad statements about what data was involved because the answer varies by individual customer and is dependent on customer choice or district policies and requirements. We continue to prioritize transparent and direct communication with our customers and our shared communities, and remain committed to providing accurate and transparent updates as more information becomes available. We want to again extend our gratitude to our customers and the students, families and educators we serve. We are dedicated to using this incident as an opportunity to grow stronger and build greater resilience as a company.

What Happened

On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration of personal information from certain PowerSchool Student Information System (SIS) environments through one of our community-focused customer support portal, PowerSource. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers. We have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.

Identity Protection & Credit Monitoring Services

PowerSchool has engaged TransUnion and Experian, trusted credit reporting agencies, to offer two years of complimentary identity protection services, which will be provided by Experian, for all students and educators whose information from your PowerSchool SIS was involved. PowerSchool will also be offering two years of complimentary credit monitoring services, which will be provided by TransUnion for all students and educators who have reached the age of majority whose information was involved. This service is being provided by TransUnion because Experian does not offer credit monitoring in Canada.

Starting in the next few weeks, PowerSchool will coordinate with TransUnion and Experian, to provide notice on behalf of our customers to students, parents / guardians and educators, as applicable, whose information was involved, as well as a call center to answer questions from the community.

Student and Educator Data Involved

For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Insurance Number (SIN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base.

Who Was Affected

On January 7, 2025, we proactively communicated this incident to the PowerSchool SIS customers affected by this incident. From January 17-24, 2025, PowerSchool shared next steps with those same SIS customers. Districts and schools that do not utilize PowerSchool SIS were not affected.

Steps We Are Taking in Response & Moving Forward

As soon as we learned of the incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. Since then, over the last few weeks, we have been focused on assessing the scope of data involved, making further enhancements to our cybersecurity defenses, and developing a plan to help you and our shared community. We take our responsibility to protect student, family, and educator data privacy extremely seriously, and we are committed to providing customers, families, and educators with resources and support as we work through this together.

General FAQ

What happened?

On December 28, 2024, we became aware of a potential cybersecurity incident involving unauthorized access to certain PowerSchool SIS information through one of our community-focused customer portals, PowerSource. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers. We have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.

When will PowerSchool provide next steps to schools, educators and families?

We are working to complete our investigation of the incident and are coordinating with districts and schools to provide more information and resources (including credit monitoring or identity protection services if applicable) as they become available.

What steps are you taking to prevent this from happening again?

PowerSchool is committed to protecting the security and integrity of our applications and regularly reviews and enhances its security policies and practices. We continue to prioritize and invest significantly in our cybersecurity defenses.

What is the timeline for providing notification information to schools, educators and families?

As PowerSchool is working to complete our investigation, we are also taking steps to set up a system – in coordination with our customers – to be able to provide supportive resources (including credit monitoring or identity protection services if applicable) for individuals whose data may have been involved. As we have more definitive information on our timeline, we will share that accordingly.

FAQ for Families

Who is PowerSchool?

PowerSchool provides cloud-based software to K-12 schools. This security incident affected some of the districts using the PowerSchool Student Information System product. We have no evidence that any other PowerSchool products were affected as a result of this incident.

Am I required to reach out to my school or take any steps as a parent or guardian at this time?

No. If you are a parent or guardian of a student under the age of majority and your student's information was exfiltrated from their district's PowerSchool SIS, you may receive a notification email from PowerSchool. Additionally, we have posted on our website and distributed a media release informing individuals of the incident and resources we have offered.

Was any student or family data involved in this incident?

For involved current and former students, and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Insurance Number (SIN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base. The notice received by involved individuals for whom we have sufficient contact information includes a description of the categories of personal information that were exfiltrated and the identity protection and credit monitoring services offered (as applicable). All the information regarding the activation of and access to these services will be included in the email sent to you by Experian. You may also visit [our website](#) linked here for information on how to activate these services

Was credit card or banking information involved in this incident?

We have no evidence that credit card or banking information was involved.

Will I get identity protection or credit monitoring?

PowerSchool is offering complimentary identity protection and credit monitoring services to all students and educators whose information from your PowerSchool SIS was involved. This offer is being provided regardless of whether an individual's Social Security number was exfiltrated.

- **Identity Protection:** PowerSchool will be offering two years of complimentary identity protection services, which will be provided by Experian, for all students and educators whose information was involved.
- **Credit Monitoring:** PowerSchool will also be offering two years of complimentary credit monitoring services, which will be provided by TransUnion, for all students and educators who have reached the age of majority whose information was involved.

Credit monitoring agencies do not offer credit monitoring services for individuals under the age of majority. If a parent / guardian enrolls an individual under the age of majority in the offered identity protection services, the individual, upon reaching the age of majority, will have the opportunity to enroll in credit monitoring services for the duration of the two-year coverage period.

Would PowerSchool reach out to me directly to request my personal information?

PowerSchool is committed to keeping our community informed and will be providing further resources as they become available. However, please remain vigilant as PowerSchool will never contact you by phone or email to request your personal or account information.

FAQ for Educators

Was any educator data involved in this incident?

For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Insurance Number (SIN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base. The notice received by each individual will include a description of the categories of personal information that were exfiltrated and the identity protection and credit monitoring services offered (as applicable).

Was credit card or banking information involved in this incident?

We have no evidence that credit card or banking information was involved.

Is PowerSchool offering identity protection and credit monitoring services?

PowerSchool has offered two years of complimentary identity protection services for all current and former students and educators whose information was determined to be involved and two years of complimentary credit monitoring services for all students and educators who have reached the age of majority and educators whose information was determined to be involved. Please visit our website [notice] for information on how to activate the services. We are doing this regardless of whether an individual's Social Insurance Number was exfiltrated.

How many districts and schools were involved?

We are not sharing specifics around the number of districts and schools we believe were involved. We are in communication with those customers directly and are supporting them through next steps.

FAQ for Customers

Was data from my school district involved?

We have proactively contacted the SIS customers that we believe were affected. If you are not a SIS customer, you were not affected.

Should we take any action to secure our own systems?

We do not believe there is an ongoing risk to our systems. We have no evidence of malware or continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers.

Were other PowerSchool products affected?

Other than PowerSchool SIS, we have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.

How will students and educators be notified if their information was involved?

PowerSchool will publish the notice on its website, circulate the notice to local media, and send the notice to email addresses, where available, of involved individuals.

The notice received by each individual will include a description of the categories of personal information that were exfiltrated and the identity protection and credit monitoring services offered (as applicable). We will also provide you a link to the notification if you would like to share with your community. Experian will also provide a call center to answer questions from the community.

Exhibit C

PowerSchool Community > Roadmap > PowerSchool SIS Technical Contacts Only
> PowerSchool SIS Self Service Student/ Staff Detail and Summary Reports Plugin

Audience

This article is intended for PowerSchool SIS Administrators with plugin installation permissions. Functions introduced by the plugin will work for both Hosted and On-Premise (Self-hosted) customers, for US and Canada.

Summary

To support our customers, PowerSchool has created a Self-Service plugin tool for customers to install, that will generate detailed and summary information that could be beneficial to you. This tool will query and summarize live PowerSchool SIS data and may not precisely reflect data that was exfiltrated at the time of the incident.

This Self-Service plugin tool can be utilized by both Hosted and On Premise (Self-Hosted) customers and details of the plugin are shared below.

- On-Premise (Self-hosted) Customers: Use of this Self-Service plugin tool is required to generate the reports needed to complete the Opt-In process. To Opt-in, you will need to confirm this, by creating a Case with Support, by February 7, 2025 and the support team will work with you through this process. The steps on creating a case can be found [in this Community article](#).
- Hosted Customers: Note that this Self-Service plugin tool, while not required for any regulatory or individual notification purposes, could be helpful in assisting you in gaining greater visibility to data that was potentially exfiltrated.

Minimum SIS Version:

This Self-Service plugin tool has been tested for use on PowerSchool SIS 23.12.0.1 or greater, however it may work on lower versions but was not tested.

Security Considerations

Page level security: After installing the Self-Service plugin tool, SIS Admin should set `/admin/powerschool/reports/summary.html` to be allowed to admin users only. See [Page-Level Permissions](#) in the product documentation.

Navigation: The page that is inserted is NOT inserted into the product navigation bar. It is, instead, a page that must be directly navigated to access.

External Connectivity: This Self-Service plugin tool only creates and sets up the necessary permissions for the reports. It does not create any external access to the reports or data, such as API OAUTH credentials.

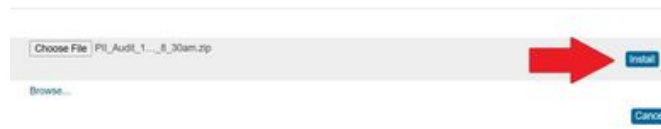
Self-Service plugin tool Installation Process Guide

1. Download the plugin (attached)
 - Do not unzip the file
 - Make note of where the file downloads
2. Log into SIS
3. Go to District Office
4. Navigate to the Plugin Configuration page (System Management > Server > Plugin Configuration)
5. Click Install.
 - Click Choose File

Plugin Install



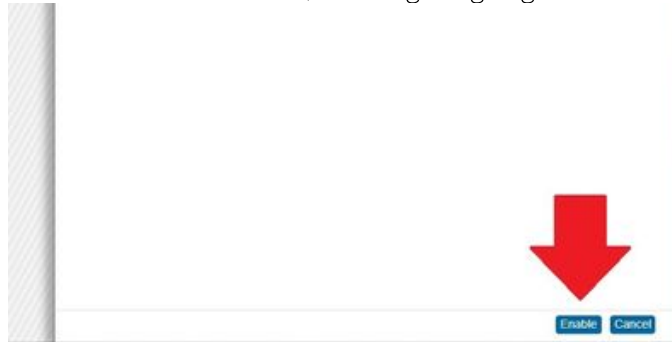
-
- Select the Plugin
- Click Install



6. Once that is installed, enable the plugin
 - Use the page search bar and search for "Powerschool Student and Staff Reports"
 - Click the checkbox next to enable



-
- A slide out will be shown, showing usage agreement. Confirm enabling



-
7. The plugin is now enabled.
 8. Ensure that customizations are enabled at System Management > Customizations> Enable Customization

Self-Service plugin tool Use

The Self-Service plugin tool introduces a new page to access a summary page and button to select and trigger the various reports. To access the page, an admin user **must be at District Office** and navigate to the page by placing /admin/powerschool/reports/summary.html in the address bar, after the end of the powerschool server address.

Only user groups that the administrator has granted access to, using page level permissions, should access and use this report.

Examples:

- Hosted SIS customer:
<https://myhostedSIS.powerschool.com/admin/powerschool/reports/summary.html>
- On Premise Customer: <https://your.domain.com/admin/powerschool/reports/summary.html>

The page provides:

- An overview of the data that is being audited. There are two tables presented:
- US - reflective of records that are associated with a valid United States state or military state designation
- Other - reflective of records that are associated with an address other than a valid United States state or military state designation

Audit table containing the following columns:

- Country – USA, CAN, or Other. Also identifies total record counts
- State or State/Province - identifies states or province
- Type – Identifies the records type (student, staff, or both)
- # Unique records - Count of unique records per Type
- # SSN/SIN field populated - Count of unique records with SSN/SIN fields populated that meet the criteria stated in the "SSN" or "SIN" description (as applicable)
- # Alert Medical field populated - Count of unique records with the Alert_Medical field populated
- # DoB field populated - Count of unique records with the Date of Birth field populated with a date in a valid DOB format
- # SSN AND/OR Alert Medical field populated - Count of unique records with one or both of SSN/SIN or Medical Alert field(s) populated (e.g., if one individual has data in both SSN/SIN and Medical Alert fields, that is counted as 1 record). For SSN/SIN to be included, it must meet the criteria stated in the "SSN" or "SIN" description (as applicable)
- # SSN AND/OR Alert Medical AND/OR DoB field populated - Count of unique records with one, two, or all three of SSN/SIN, Medical Alert, or Date of Birth field populated (e.g., if one individual has data in all of SSN/SIN, Medical Alert, and Date of Birth fields, that is counted as 1 record). For SSN/SIN to be included, it must meet the criteria stated in the "SSN" or "SIN" description (as applicable)

Additional explanation regarding the Glossary provided in the Plugin:

USA Table

- # Unique Records – Count of unique records with any field populated
- # SSN field populated – Count of unique records with SSN field populated with a 9 digit number that meets criteria for being a valid US SSN
- # Alert Medical field populated – Count of unique records with Alert_Medical field populated
- # DOB field populated – Count of unique records with the Date of Birth field populated with a date in a valid DOB format
- # SSN and/or Alert Medical field populated – Count of unique records with one or both of SSN or Alert Medical field(s) populated (e.g., if one individual has data in both SSN and Alert Medical fields, that is counted as 1 record). For SSN to be included, it must meet the criteria stated in the "# SSN field populated" description
- # SSN and/or Alert Medical and/or DOB field populated - Count of unique records with one, two, or all three of SSN, or Alert Medical, or Date of Birth field(s) populated (e.g. if one individual has data in all of SSN, Alert Medical, and Date of Birth fields, that is counted as 1 record). For SSN to be included, it must meet the criteria stated in the "# SSN field populated" description.

Canada / Other Table

- # Unique Records – Count of unique records with any field populated
- # SIN field populated - Count of unique records with SSN field populated with a 9 digit number
- # Alert Medical field populated – Count of unique records with Alert_Medical field populated

- # DOB field populated– Count of unique records with the Date of Birth field populated with a date in a valid DOB format
- # SIN and/or Alert Medical field populated - Count of unique records with one or both of SSN or Alert Medical field(s) populated (e.g. if one individual has data in both SSN and Alert Medical fields, that is counted as 1 record). For SSN to be included, it must meet the criteria stated in the "# SIN field populated" description.
- # SIN and/or Alert Medical and/or DOB field populated - Count of unique records with one, two, or all three of SSN or Alert Medical, or Date of Birth field(s) populated (e.g. if one individual has data in all of SSN, Alert Medical, and Date of Birth fields, that is counted as 1 record). For SSN to be included, it must meet the criteria stated in the "# SIN field populated" description.

Download links for the following series of reports (CSV format) with both US and non-US versions:

- Staff & Student Summary Report – an extracted report of data as represented on the screen.
- Staff Detail Report: CUSTOMER NUMBER, TYPE, FIRST NAME, LAST NAME, SCHOOL NAME, YEAR OF BIRTH, STATE, NOTIFICATION EMAIL (On-prem will be filled to facilitate individual notification), DOB POPULATED (Y/N), POSSIBLE SSN/SIN[Footnote] (Y/N)
- Student Detail Report: CUSTOMER NUMBER, TYPE FIRST NAME, LAST NAME, SCHOOL NAME, YEAR OF BIRTH, STATE, NOTIFICATION EMAIL (On-prem will be filled to facilitate individual notification), LOG_CREATION_DATE, FIRST ENTRY DATE, LAST EXIT DATE, ALERT MEDICAL POPULATED (Y/N), DOB POPULATED (Y/N), POSSIBLE SSN/SIN[Footnote] (Y/N)

Although not restricted to use outside of the District Office, these are district level reports. ***This report should only be run from District Office.***

Generating reports from the Self-Service plugin tool page

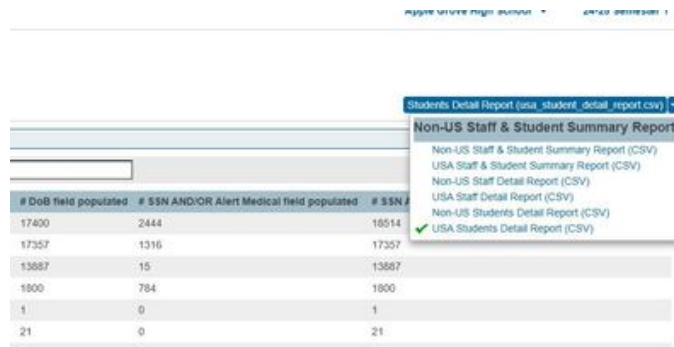
1. Login to SIS
2. Go to District Office
3. In the address bar, replace /admin/powerschool/reports/summary.html at the end of the SIS URL
 - Example: <https://mypowerschool.com/admin/powerschool/reports/summary.html>
4. On the top right side of the audit output table, click the dropdown arrow

Summary Data Report



Customer	Type	First Name	Last Name	School Name	Year of Birth	State	Notification Email	DOB Populated	Possible SSN/SIN	Alert Medical
10001	Student	John	Doe	ABC School	1990	CA	john.doe@abc.edu	Y	Y	N
10002	Student	Jane	Doe	ABC School	1991	CA	jane.doe@abc.edu	Y	Y	N
10003	Student	John	Smith	ABC School	1992	CA	john.smith@abc.edu	Y	Y	N
10004	Student	Jane	Smith	ABC School	1993	CA	jane.smith@abc.edu	Y	Y	N
10005	Student	John	Johnson	ABC School	1994	CA	john.johnson@abc.edu	Y	Y	N
10006	Student	Jane	Johnson	ABC School	1995	CA	jane.johnson@abc.edu	Y	Y	N
10007	Student	John	Williams	ABC School	1996	CA	john.williams@abc.edu	Y	Y	N
10008	Student	Jane	Williams	ABC School	1997	CA	jane.williams@abc.edu	Y	Y	N
10009	Student	John	Miller	ABC School	1998	CA	john.miller@abc.edu	Y	Y	N
10010	Student	Jane	Miller	ABC School	1999	CA	jane.miller@abc.edu	Y	Y	N
10011	Student	John	Wilson	ABC School	2000	CA	john.wilson@abc.edu	Y	Y	N
10012	Student	Jane	Wilson	ABC School	2001	CA	jane.wilson@abc.edu	Y	Y	N
10013	Student	John	Moore	ABC School	2002	CA	john.moore@abc.edu	Y	Y	N
10014	Student	Jane	Moore	ABC School	2003	CA	jane.moore@abc.edu	Y	Y	N
10015	Student	John	Taylor	ABC School	2004	CA	john.taylor@abc.edu	Y	Y	N
10016	Student	Jane	Taylor	ABC School	2005	CA	jane.taylor@abc.edu	Y	Y	N
10017	Student	John	Anderson	ABC School	2006	CA	john.anderson@abc.edu	Y	Y	N
10018	Student	Jane	Anderson	ABC School	2007	CA	jane.anderson@abc.edu	Y	Y	N
10019	Student	John	Thomas	ABC School	2008	CA	john.thomas@abc.edu	Y	Y	N
10020	Student	Jane	Thomas	ABC School	2009	CA	jane.thomas@abc.edu	Y	Y	N
10021	Student	John	Clark	ABC School	2010	CA	john.clark@abc.edu	Y	Y	N
10022	Student	Jane	Clark	ABC School	2011	CA	jane.clark@abc.edu	Y	Y	N
10023	Student	John	Lewis	ABC School	2012	CA	john.lewis@abc.edu	Y	Y	N
10024	Student	Jane	Lewis	ABC School	2013	CA	jane.lewis@abc.edu	Y	Y	N
10025	Student	John	Walker	ABC School	2014	CA	john.walker@abc.edu	Y	Y	N
10026	Student	Jane	Walker	ABC School	2015	CA	jane.walker@abc.edu	Y	Y	N
10027	Student	John	Hall	ABC School	2016	CA	john.hall@abc.edu	Y	Y	N
10028	Student	Jane	Hall	ABC School	2017	CA	jane.hall@abc.edu	Y	Y	N
10029	Student	John	Young	ABC School	2018	CA	john.young@abc.edu	Y	Y	N
10030	Student	Jane	Young	ABC School	2019	CA	jane.young@abc.edu	Y	Y	N
10031	Student	John	King	ABC School	2020	CA	john.king@abc.edu	Y	Y	N
10032	Student	Jane	King	ABC School	2021	CA	jane.king@abc.edu	Y	Y	N
10033	Student	John	Wright	ABC School	2022	CA	john.wright@abc.edu	Y	Y	N
10034	Student	Jane	Wright	ABC School	2023	CA	jane.wright@abc.edu	Y	Y	N
10035	Student	John	Scott	ABC School	2024	CA	john.scott@abc.edu	Y	Y	N
10036	Student	Jane	Scott	ABC School	2025	CA	jane.scott@abc.edu	Y	Y	N

5. Select which report needs to be run



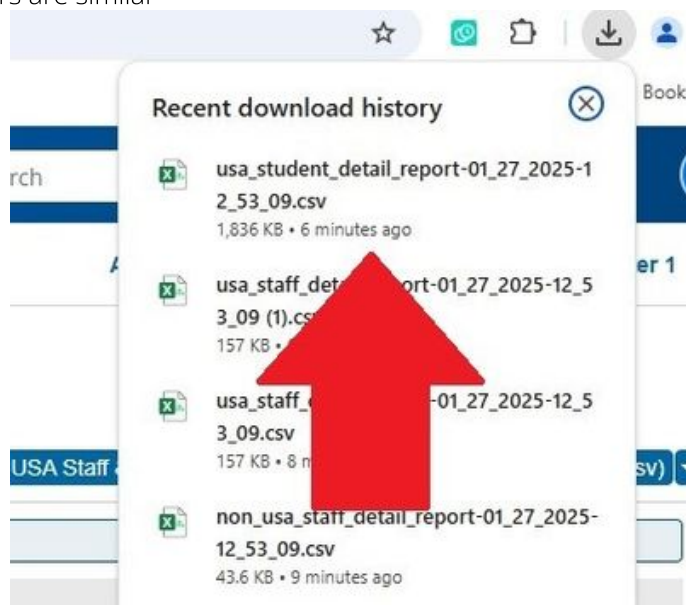
# DoB field populated	# SSN AND/OR Alert Medical field populated	# SSN AND/OR Alert Medical AND/OR DoB field populated
17400	2444	18514
17357	1316	17357
13887	15	13887
1900	784	1900
1	0	1
21	0	21

6. Click the report name in the blue bar again



# SSN AND/OR Alert Medical field populated	# SSN AND/OR Alert Medical AND/OR DoB field populated
2444	18514

7. Files are generated and automatically downloaded through the browser. Chrome browser show, others are similar

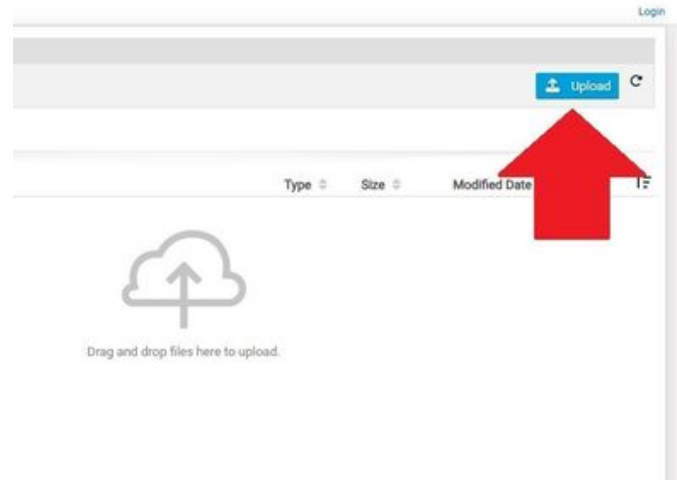


8. Go to your downloads folder, or wherever your downloads are targeted to go.

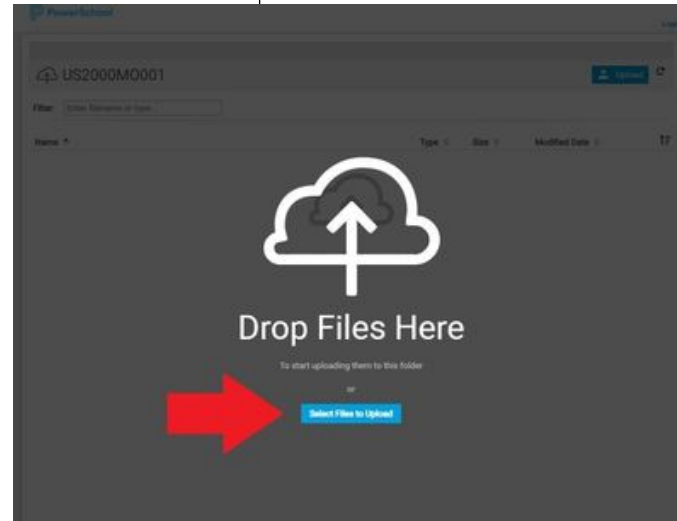
9. Open report file with the spreadsheet program of choice to review the data.

PLEASE DO NOT ATTACH A DATA FILE TO THE SUPPORT CASE**Submitting the report output files to PowerSchool (US and Non-US Opt-In On-Premises Customers ONLY)****Submitting the report output files to PowerSchool**

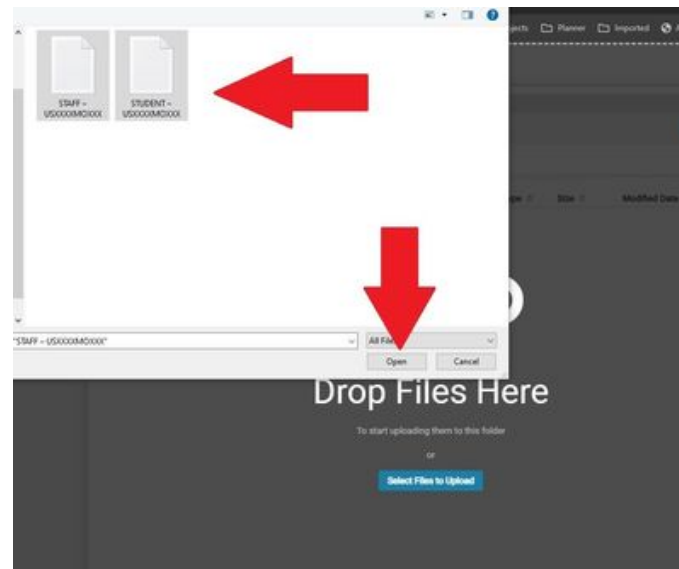
1. Generate and download both Staff and Student Detail Reports (see steps under Generating reports from the Self-Service plugin tool page)
2. Open in a spreadsheet program
 - If the file opens in the spreadsheet program, but doesn't put the data into separate columns, use the programs text to columns function
 - In Excel, click the column with all the data
 - Switch to the data tab
 - Select text to column
 - Set the delimiter to comma
 - Process the change
3. Validate email addresses to make sure that they are accurate.
4. Save the files with the following naming format:
 - US customers
 - usa_staff_detail_report-mm_dd_yyyy-hh_mm_ss
 - usa_student_detail_report-mm_dd_yyyy-hh_mm_ss
 - Non-US customers
 - non_ usa_staff_detail_report-mm_dd_yyyy-hh_mm_ss
 - non_ usa_student_detail_report-mm_dd_yyyy-hh_mm_ss
5. In the case with support, request a Datto upload link
 - Support provides the link and password to upload in two secure emails
 - Upload the file to the Datto folder
 - US and Non-US, excluding CA customers will be provided a US based Datto link
 - CA customers will be provided a CA based Datto link
 - Access the Support provided Datto upload link
 - Enter the password
 - Click the upload button



-
- Click select files to upload



-
- Select both Staff Preferred Email and Student Preferred Email extracts and click the open button



- 6. The upload process starts immediately
- 7. When complete, you should see a screen that looks like this



- 8. Verify BOTH files uploaded. Once you exit this screen, you will not be able to view what files are present
- 9. After confirmation, notify support, via case comment, that the upload is completed.
- 10. Support will verify that two files are uploaded and communicate any needed next steps. for verification

PLEASE DO NOT ATTACH A DATA FILE TO THE SUPPORT CASE

Plugin Download is available [here](#).

This will take you to Powersource, where you will need to login. This file download is restricted to Technical Contacts.





Exhibit D

Investigation Report

PREPARED FOR

PowerSchool Group LLC

DELIVERED ON

February 28, 2025



Table of Contents

Executive Summary	3
Background	3
Objectives	3
Scope	4
Key Findings	5
Investigative Methodology	7
Falcon Forensics Collector (FFC)	7
CrowdStrike Falcon	8
Log Analysis	8
Microsoft Azure	9
Appendix A: Indicators of Compromise	11



Executive Summary

Background

On December 28, 2024, PowerSchool identified suspicious activity using credentials belonging to a support user (“compromised support credentials”) in their PowerSchool Student Information System (SIS).¹ On December 29, 2024, CrowdStrike Services (“CrowdStrike”) was engaged to provide investigative services and to assess the scope and extent of unauthorized third party (“Threat Actor”) activity in the PowerSchool environment. CrowdStrike’s investigation began on December 29, 2024, and concluded on February 17, 2025.

CrowdStrike is informed that following the security incident, PowerSchool took steps to prevent the data involved from further unauthorized access or misuse and to secure the impacted environment. CrowdStrike understands this involved:

- Deactivating the compromised credential
- Enforcing a full password reset for employees and contractors
- Restricting access to and tightening password and access controls for the affected customer support portal
- Requiring that access to the PowerSource environment be via company’s VPN, which requires single sign-on (SSO) and multi-factor authentication (MFA)

In conducting the review, CrowdStrike observed that PowerSchool’s endpoints and servers are protected by CrowdStrike’s Falcon Endpoint Detection and Response (EDR) software, which provides advanced security monitoring, threat detection, next-generation antivirus, and real-time endpoint detection and response (EDR) capabilities. PowerSchool’s systems are also protected by CrowdStrike’s Falcon Overwatch, a 24/7/365 threat hunting service. In addition, CrowdStrike is informed that PowerSchool’s systems and data storage was configured with AES-256 encryption for data at rest.

Objectives

CrowdStrike’s objectives were to determine the following:

- How the Threat Actor gained access to the PowerSchool environment.
- The earliest and most recent dates of Threat Actor activity.
- Whether the Threat Actor moved laterally in the PowerSchool environment and, if so, how.
- Whether there was any evidence that the Threat Actor accessed or exfiltrated PowerSchool data and, if so, what data was accessed or exfiltrated.

¹ Per PowerSchool’s website, PowerSchool SIS “provides back-office administrator functionality, as well as student-, parent- and faculty-facing functionality to manage key organizational information assets, including demographic data, enrollment, grades, transcripts, and other governmental agency reporting capabilities.” See <https://www.powerschool.com/operations/student-information-systems/>.



- Whether the Threat Actor persists in the PowerSchool environment, or whether they have been evicted.

Scope

CrowdStrike's scope in the investigation involved performing the following:

- Review and monitoring of CrowdStrike Falcon ("Falcon") data.
- Review of Falcon Forensics Collector (FFC) data.
- Analysis of additional logs provided by PowerSchool.



Key Findings

The following is a summary of the key findings from CrowdStrike's analysis of available data.

1. **The earliest evidence of unauthorized activity attributable to the Threat Actor within the PowerSchool environment occurred on December 19, 2024, at 04:06:24 UTC.**

At that time, the Threat Actor initiated an HTTP GET request for `support.powerschool[.]com` from IP address `146.70.128[.]186`.

2. **The Threat Actor performed Maintenance Remote Support operations in PowerSource to gain access to PowerSchool customers' SIS data.**

Between December 19, 2024, at 19:43:14 UTC, and December 28, 2024, at 06:31:18 UTC, the Threat Actor performed Maintenance Remote Support operations in PowerSource, which enabled the Threat Actor to access the individual customer organizations' SIS instances. At 19:43:37 UTC, the Threat Actor initiated a Maintenance Remote Support connection to PowerSchool SIS from the same IP address using the compromised support credentials. Per PowerSchool's website, "PowerSource is a community-focused customer support portal for all PowerSchool products."² As such, PowerSource allows a support technician with sufficient permissions to gain access to customer SIS database instances for maintenance purposes.

3. **The Threat Actor exfiltrated data from the PowerSchool SIS instances of PowerSchool customers.**

Between December 19, 2024, at 23:02:54 UTC, and December 23, 2024, at 08:04:45 UTC, the Threat Actor exfiltrated data from the `Teachers` and `Students` tables of the PowerSchool SIS instances for certain PowerSchool customers; CrowdStrike found no evidence of data exfiltration from any other tables.

4. **CrowdStrike found no evidence of access or escalation of privilege by the Threat Actor to any PowerSchool systems beyond application-level access via the web-based interface.**

CrowdStrike has found no evidence of system-layer access or malware associated with this incident. CrowdStrike also examined the tactics, techniques and procedures associated with the Threat Actor, as well as their actions taken in this incident, and did not identify any indications that PowerSchool customer IT environments outside of PowerSource and SIS were compromised or were at risk of intrusion due to this incident.

5. **CrowdStrike identified earlier evidence of unauthorized activity in the PowerSchool environment associated with the compromised support credentials between August 16, 2024 and September 17, 2024.**

Beginning on August 16, 2024, at 01:27:29 UTC, PowerSource logs showed that an unknown actor successfully accessed the PowerSchool PowerSource portal using the compromised support credentials. CrowdStrike did not find sufficient evidence to attribute this activity to the Threat Actor responsible for the activity in December 2024. The available SIS log data did not go back far enough to show whether the August and September activity included unauthorized access to PowerSchool SIS data.

² <https://support.powerschool.com/>



6. The most recent evidence of Threat Actor activity in the Customer environment occurred on December 28, 2024, at 06:31:18 UTC.

At that time, the Threat Actor used the compromised support credentials to log in to the maintenance interface of PowerSource to interact with PowerSchool SIS.

7. CrowdStrike's dark web monitoring did not identify exfiltrated data for sale related to this incident.

PowerSchool engaged CrowdStrike's Recon+ Intelligence service as of January 2, 2025, to engage in dark web monitoring, and, as of the date of this report, CrowdStrike has not identified any evidence of information exfiltrated in this incident being made available for sale or download.



Investigative Methodology

CrowdStrike uses a combination of tools and investigative techniques to perform forensic and triage analysis of system and network data. This section provides an overview of those tools, techniques, and procedures followed in CrowdStrike's investigative methodology.

Falcon Forensics Collector (FFC)

FFC gathers artifacts from servers and workstations to support incident response triage, and compromise assessment analysis. This proprietary CrowdStrike tool implements data gathering modules and collects incident response-relevant data from the host. The tool places the data it collects into a database for CrowdStrike consultants to analyze en masse. FFC can collect numerous different types of system data to investigate present or historical threat actor activity. Data types collected by FFC include, but are not limited to, the following:

Microsoft Windows

- Disk Artifacts
 - Directory listing: A listing of targeted files from file paths on each host
 - File hashes: MD5 hashes of the files collected in the directory listing
 - Portable executable information: File metadata
 - Application Compatibility Cache: Execution tracked by legacy compatibility check
 - Prefetch and SuperFetch: Operating system (OS) optimization for frequently used files
 - Registry data: Forensically interesting keys and values from host registry hives
 - Event logs: Significant OS security, application, and system events
- Volatile System Information
 - Running processes: Processes that are currently running on the host
 - Shares: Mapped network folder shares
 - Network connections: Current network connections of the host
 - Domain Name System (DNS) cache: Volatile data on domain lookups stored for future use
- System Configuration
 - Scheduled tasks: Scheduled commands or batch scripts
 - Services: All services present on host
 - Users
 - Persistence locations



Linux/UNIX

- Disk Artifacts
 - Directory listing: A listing of all files from file paths on each host
 - File hashes: MD5 hashes of the files collected in the directory listing
 - Configuration data: Forensically interesting values from host configuration locations
 - Log data: Various logs in `/var/log` and `/var/adm`
- Volatile System Information
 - Running processes: Processes that are currently running on the host
 - Shares: Mapped network folder shares
 - Network connections: Current network connections of the host
- System Configuration
 - Cron Jobs: Scheduled commands or batch scripts
 - Persistence Locations
 - Services: All services present on host
 - Users

CrowdStrike Falcon

CrowdStrike Falcon is a suite of endpoint protection technologies that provide advanced security monitoring, threat detection, next-generation antivirus, and real-time endpoint detection and response (EDR) capabilities. Falcon continuously monitors and collects details of OS activity, such as process execution metadata, so that it can be analyzed for behavioral and threat intelligence-led indicators of attack.

During an Incident Response investigation, CrowdStrike uses this real-time telemetry to detect potential Threat Actor activity based on behavioral indicators of attack, indicators of compromise, and active threat hunting. CrowdStrike leveraged Falcon to triage potentially suspicious events and perform analysis on a system to determine if that behavior is malicious.

Log Analysis

CrowdStrike gathers or obtains access to relevant logs to support incident response investigations. Available log sources are identified, and the timeline of available data is documented. CrowdStrike consultants use a combination of tool-based analysis, en masse log searching, and manual event reviewing techniques to seek anomalous data in available log sources, indicative of attempts to attack a computer network or system.

CrowdStrike analyzed a variety of log sources, including but not limited to:

- Logs from network appliances:
 - Firewalls and Next Generation Firewalls (NGFWs)



- Network connections
 - Network disconnections
 - Network traffic & NetFlow data
- Web Application Firewalls
 - Connection data
 - HTTP access logs
- Application Load Balancers
 - Connection data
 - HTTP access logs
- Web logs from Linux web servers
 - Access logs
 - Error logs
 - Catalina application logs
- Audit logging generated by the web applications that were the subject of unauthorized access

Microsoft Azure

CrowdStrike's Azure incident response methodology includes an assessment of available log sources, and subsequent, targeted collection and analysis of available logs for evidence of Threat Actor activity. Analysis is performed as per the MITRE ATT&CK taxonomy, with activity grouped into Threat Actor initial access, privilege escalation, lateral movement, and/or additional impact.

CrowdStrike's investigation also includes an evaluation of the Azure control plane configuration against a secure baseline, recognized by CrowdStrike as critical in defending against modern cloud security threats.

CrowdStrike may review any of the following key Azure components, where investigation-relevant log data is available, using a combination of automated and manual analysis techniques:

- Azure Infrastructure as a Service (IaaS) and Active Directory Logging
 - Azure Active Directory (AD) Interactive Sign-in logs
 - Azure AD Non-Interactive Sign-in logs
 - Azure Service Principal Sign-in logs
 - Azure Managed Identity Sign-in logs
 - Azure AD Audit logs
 - Azure Subscription Activity logs
 - Azure Service Bus logs
 - Azure API Management logs
 - Azure Load Balancing type service logs



- Azure Network Security Group Flow logs
 - Azure Storage Account logs
- Identity and Access Management and Encryption
 - Azure Active Directory
 - Azure Key Vault
- Security Monitoring and Alerting
 - Azure Security Center
 - Azure Identity Protection



Appendix A: Indicators of Compromise

Table 1 provides a summary of the system- and network-based indicators of compromise (IOCs) that CrowdStrike identified in the environment.

Indicator	Indicator Type	Description
91.218.50[.]11	IP Address	This IP is associated with data exfiltration from PowerSchool SIS in December 2024.
146.70.128[.]165	IP Address	This IP is associated with data exfiltration from PowerSchool SIS in December 2024.
96.44.191[.]140	IP Address	This IP is associated with data exfiltration from PowerSchool SIS in December 2024.
169.150.203[.]39	IP Address	This IP is associated with PowerSource activity in December 2024 .
185.213.154[.]172	IP Address	This IP is associated with PowerSource activity in December 2024 .
193.32.127[.]248	IP Address	This IP is associated with PowerSource activity in December 2024 .
66.63.167[.]173	IP Address	This IP is associated with PowerSource activity in December 2024 .
146.70.128[.]186	IP Address	This IP is associated with PowerSchool SIS activity in December 2024 .
193.32.162[.]96	IP Address	This IP is associated with PowerSchool SIS activity in December 2024 .
146.70.174[.]52	IP Address	This IP is associated with PowerSchool SIS activity in December 2024 .

Table 1: Indicators of Compromise