PowerSchool
Personalized Education for Every Journey

PowerSchool Cybersecurity Incident – Customer FAQs

1. What happened?

On December 28, 2024, we 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 SIS customer data using a compromised credential.

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.

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.

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.

We are promptly notifying affected SIS customers and will be working diligently with them to communicate with their educators, families, and other stakeholders.

2. When did you find out that this happened?

On December 28, 2024, we 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 SIS customer data using a compromised credential.

3. Was data stolen?

On December 28, 2024, we 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 SIS customer data using a compromised credential.

4. Was this ransomware?

No.

5. What steps have you taken to confirm that the data in question has since been deleted in its entirety?

Given the sensitive nature of our investigation, we are unable to provide information on certain specifics.

However, 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.

PowerSchool engaged the services of CyberSteward, a professional advisor with deep experience in negotiating with threat actors. With their guidance, PowerSchool has received reasonable assurances from the threat actor that the data has been deleted and that no additional copies exist.

6. Are your operations affected?

PowerSchool is not experiencing, nor expects to experience, any operational disruption and continues to provide services as normal to our customers.

7. How are you responding to this incident?

On December 28, 2024, we 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 SIS customer data using a compromised credential.

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 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.

As part of our ongoing efforts to enhance our resilience, we have further strengthened PowerSource password policies and controls including increasing password length and complexity requirements. We continue to prioritize and invest significantly in our cybersecurity defenses.

We are promptly notifying affected SIS customers and will be working diligently with them to communicate with their educators, families, and other stakeholders. PowerSchool is committed to supporting our customers and is equipped to conduct a thorough notification process to all impacted individuals. Over the coming weeks, we will partner directly with our impacted customers on the details of this notification process.

We are also promptly notifying non-impacted SIS and general PowerSchool customers. No action will be required by these customers, as their data and/or products were not impacted.

In the coming days, PowerSchool will be providing affected customers with a communications package to support them 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 teams can confidently discuss this incident with their communities.

We are addressing the situation in an organized and thorough manner, following all of our incident response protocols. PowerSchool is committed to providing affected customers with the resources and support they may need as we work through this together.

8. How confident are you that the incident has been contained?
The incident is contained, and we have no evidence of malware or continued unauthorized activity in the PowerSchool environment.

9. What steps are you taking to prevent this from happening again?
As part of our ongoing efforts to enhance our resilience, we have further strengthened PowerSource password policies and controls including increasing password length and complexity requirements. We continue to prioritize and invest significantly in our cybersecurity defenses.

10. Are schools that use your services experiencing disruptions as a result of this?
No. PowerSchool is not experiencing, nor expects to experience, any operational disruption and continues to provide services as normal to our customers.

11. How many customers were affected by this incident? How many students and teachers in total were affected?
Given the sensitive nature of our investigation, we are unable to provide information on certain specifics.

However, we want to reiterate that the unauthorized access point was isolated to our PowerSource portal. Only the SIS database can be accessed from the PowerSource portal, and we can confirm the information accessed belongs to certain SIS customers and relates to families and educators.

12. Will you be notifying all impacted individuals?
We are promptly notifying affected SIS customers and will be working diligently with them to communicate with their educators, families, and other stakeholders. PowerSchool is committed to supporting our customers and is equipped to conduct a thorough notification process to all impacted individuals. Over the coming weeks, we will partner directly with our impacted customers on the details of this notification process.

13. Was data from my school district exposed?
We have proactively contacted the SIS customers that we believe may have had data impacted. If you are not a SIS customer, you were not affected.

14. Are you providing legal notice and credit monitoring/identity theft protection for affected individuals?

In the coming days, PowerSchool will be providing affected customers with a communications package to support them 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 teams can confidently discuss this incident with their communities.

We have taken all appropriate steps to further prevent the exposure of information affected by 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.

15. Was sensitive personal information included in the affected data?

Yes. We are still working through our detailed data review for each of the impacted customers; however, we believe the export data manager tool was used to extract only student and teacher tables. These tables primarily include contact information with data elements such as name and address information. For a subset of the customers, these tables may also include Social Security Number (SSN), other Personally Identifiable Information (PII), and some medical and grades information for current and former students depending on the specific school district. PowerSchool will be providing credit monitoring to affected adults and identity protection services to affected minors whose SSN was impacted 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 formal notification obligations.

16. What types of information about parents and guardians is typically maintained in SIS?

We are still working through our detailed data review for each of the impacted customers; however, we believe the export data manager tool was used to extract only student and teacher tables. These tables may include data elements such as the parent or guardian's name, phone number, and/or email depending on the specific school district.

17. What type of information about teachers is typically maintained in SIS?

We are still working through our detailed data review for each of the impacted customers; however, we believe the export data manager tool was used to extract only teacher and student tables. These tables primarily include contact information with data elements such as name and address information. For a subset of the customers, these tables may also include Social Security Number (SSN), and other Personally Identifiable Information (PII) of current and former educators depending on the specific school district. PowerSchool will be providing credit monitoring to affected adults whose SSN was impacted 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 formal notification obligations.

18. Is it safe to continue conducting business with you? Should we be taking any action to secure our own systems?

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.

The unauthorized access point was isolated to our PowerSource portal. Only the SIS database can be accessed from the PowerSource portal, and we can confirm the information accessed belongs to certain SIS customers and relates to families and educators.

19. What steps should we take to mitigate risks to our students and staff?

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 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.

In the coming days, PowerSchool will be providing affected customers with a communications package to support them 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 teams can confidently discuss this incident with their communities.

The particular information compromised will vary by impacted customer. We anticipate that only a subset of impacted customers will have notification obligations. We will also support you in providing formal notification to affected individuals.

20. Can an incident report be provided?

Yes. CrowdStrike is finishing their analysis in the coming days, and we expect to have a finalized forensic report by January 17th which we are happy to share.