Park West School Division
Learners Today, Leaders Tomorrow

Stephen David
Superintendent/CEO

Louise Langevin
Assistant Superintendent

Date: Thursday, February 6, 2025

Topic: **PowerSchool Cybersecurity Incident**

We are writing to provide a further update about the cybersecurity incident that PowerSchool, our student information system (SIS) provider, recently experienced.

Our previous update on January 30, 2025 mentioned that PowerSchool would be providing notice to students, parents/guardians, and educators whose information was involved and that the notice would include information about identity protection and/or credit monitoring services offered. PowerSchool has now advised us that it has initiated the process of notifying those individuals.

PowerSchool will be notifying individuals by email and we understand the email will be sent from ps-sis-incident@mail.csid.com. We understand these emails will be sent by PowerSchool in the coming weeks.

Whether or not you receive an email, you may also visit PowerSchool's website to learn how to activate the identity protection and/or credit monitoring services. For those able to utilize credit monitoring services (individuals over 18), you will be prompted to validate before activating by entering your first name, last name, and date of birth. Anyone, including those under 18, can utilize the identity protection services. You may not be able to access the credit monitoring services immediately, as PowerSchool is still updating its list of eligible individuals. PowerSchool indicated that its updates should be completed by the end of February. PowerSchool has advised that you can call 833-918-7884 if you have any questions.

We continue to work diligently to request more details from PowerSchool. We also continue to investigate this incident ourselves, with assistance from experts. We may be in touch again with further updates.

There continue to be no operational impacts on Park West School Division as a result of this incident. PowerSchool has assured us that the incident has been contained.

In Park West School Division, we take cybersecurity and protecting information seriously. We will post updates about the PowerSchool cybersecurity incident on our website and social media accounts. We have previously provided some answers to questions you may have. The updated answers may be found on pages 2-3 of this document. If you have any additional questions, they can be directed to pwsdoffice@pwds.ca

Thank you for your continued understanding and patience as we navigate this situation.

FREQUENTLY ASKED QUESTIONS

The incident

1. What happened?

On January 7, 2025, PowerSchool informed Park West School Division that it had experienced a cybersecurity incident involving unauthorized access to certain customer information in late December 2024. Park West School Division is a customer of PowerSchool, like many other educational institutions across North America. PowerSchool provides a Student Information System (SIS).

PowerSchool also informed us that the unauthorized access included access to information related to Park West School Division. We await additional details from PowerSchool about the information involved and are committing to sharing details when we have them.

Whether or not you receive an email, you may also visit PowerSchool's website to learn how to activate the identity protection and/or credit monitoring services. Anyone, including those under 18, can utilize the identity protection services. You may not be able to access the credit monitoring services immediately, as PowerSchool is still updating its list of eligible individuals. PowerSchool indicated that its updates should be completed by the end of February. PowerSchool has advised that you can call 833-918-7884 if you have any questions.

We have been informed that PowerSchool has contained the incident and that there is no evidence of malware or continued unauthorized activity in the PowerSchool environment. There have been no operational impacts on Park West School Division as a result of this incident.

2. Who did this and for what purpose?

This incident occurred at PowerSchool. We await additional details about the incident from PowerSchool. Unfortunately, organizations across the public and private sectors are increasingly being impacted by incidents like this.

3. How did you respond to the incident?

Upon becoming aware of the cybersecurity incident, Park West School Division has been working diligently to investigate, to request more details from PowerSchool and ask questions about the details it has provided to date. We have also been investigating this incident ourselves, with assistance from experts. We await additional details from PowerSchool about the information accessed as a result of this incident so we can take further action.

PowerSchool has informed us that it has taken various response actions, including containing the incident, informing law enforcement, investigating the incident, conducting a full internal password reset, and tightening password for all its internal accounts.

PowerSchool is in the process of notifying Canadian regulators about this incident. Park West School Division has already notified the Manitoba Ombudsman.

4. How long will the investigation take?
PowerSchool has advised it intends to provide additional details shortly. Once we have additional details from PowerSchool, we will seek to complete our investigation as quickly as possible.

5. Has the incident been resolved?
We have been informed that PowerSchool has contained the incident and that there is no evidence of malware or continued unauthorized activity in the PowerSchool environment. There have been no operational impacts on Park West School Division as a result of this incident.

The response

6. Has law enforcement been notified?
Yes, PowerSchool has advised us that it has notified law enforcement.

7. Has the Manitoba Ombudsman been advised?
Yes, the Manitoba Ombudsman has been advised.

The impact

8. Why did this happen to Park West School Division?
PowerSchool is a vendor used by many educational institutions in North America. We are a customer of PowerSchool and, as a result of the incident experienced by PowerSchool, we were impacted. We have no reason to believe that Park West School Division was a specific target in this incident.

The data

9. Has information been accessed? Was information from Park West School Division exposed?
PowerSchool confirmed that there was unauthorized access to certain PowerSchool customer data, including data related to Park West School Division. PowerSchool's investigation is ongoing and we await additional details from PowerSchool.

Based on our own investigation to date of the information stored in our SIS, we can advise that **no parent/guardian, staff, or student Social Insurance Number (SIN), banking, or credit card information has been identified as stored in our SIS**. PowerSchool has nevertheless advised us that the identity protection and credit monitoring offers mentioned above will be sent to all individuals with *any* information involved.