SWAN VALLEY
SCHOOL DIVISION

May 5, 2025

Re: Update on PowerSchool Cybersecurity Incident

Dear Swan Valley School Division Community,

We are writing with an update on the PowerSchool cybersecurity incident. In our previous updates (https://www.svsd.ca/_ci/p/7184) about the incident, we mentioned that PowerSchool would be sending emails to students, parents/guardians, and educators whose information was involved in the incident. We understand that members of the Swan Valley School Division community have now received this email from PowerSchool and others may receive it in the coming days.

We understand from PowerSchool that the email was or will be sent from one of the following similar email addresses: ps-sis-incident@mail.csid.com; ps-sis-incident@mail1.csid.com; or ps-sis-incident@mail2.csid.com. **If you receive or have received an email from any one of these email addresses with the subject line "PowerSchool Cybersecurity Incident", we have been assured by PowerSchool that it is a legitimate email.** The email includes information about how to activate the 2 years of identity protection and/or credit monitoring services offered. Please find attached an example of what the email from PowerSchool looks like, although there may be differences between it and the one you receive.

**Whether or not you received the email from PowerSchool, you may also visit PowerSchool's website to learn how to activate the identity protection and/or credit monitoring services.** The PowerSchool website also includes information in French. For those able to utilize credit monitoring services (anyone age 18 and over), you will be prompted to validate before activating by entering your name and date of birth. Anyone, including those under 18, can utilize the identity protection services. PowerSchool has advised that you can call 833-918-7884 if you have any questions.

Please review the email from PowerSchool carefully. It includes details about the incident and the information identified by PowerSchool as involved. In the email, PowerSchool explains that, on December 28, 2024, it became aware that it experienced a cybersecurity incident involving unauthorized access to and exfiltration (acquisition) of certain personal information from PowerSchool Student Information System (SIS) environments. This occurred between around December 19 and December 28, 2024. PowerSchool also advised us that it has taken steps to prevent the information involved from further unauthorized access or misuse, that it does not anticipate the information being shared or made public, and that it believes the information has been deleted without any further replication or dissemination. Like many school institutions across North America, we use PowerSchool for our SIS and thus were informed by PowerSchool that information stored by Swan Valley School Division in our SIS was involved in the incident.

You will see that PowerSchool includes in the email a description of some of the information that was potentially involved in the incident. The information involved varies by person.

1481 Third Street N, John Kastrukoff Building
Administration Office 204-734-4531
Box 995, Swan River, MB R0L 1Z0

For students, the information involved will generally be limited to information parents/guardians provided Swan Valley School Division upon registration of their child as a student or any subsequent updates to that information. For many students, the information involved was name, date of birth, gender, phone number, address, school email address, doctor's name and phone number, MET number, school ID number, and/or enrolment/registration records as well as the parent/guardian's name and contact information. For a small number of students, there was also relevant medical information (e.g., allergies) and/or relevant alerts (e.g., related to discipline, guardian, custody, or other issues).

For staff, the information involved was name, date of birth, date of birth, gender, contact information, address, and/or school contact information.

The email from PowerSchool also refers to Social Insurance Number (SIN) as potentially involved but should also include a statement if there is no evidence that your SIN was involved – please review the email carefully. As we mentioned previously, based on our own investigation of the information stored in our SIS, **no parent/guardian, staff, or student SIN, banking, or credit card information was stored in our SIS and thus such information was NOT involved in the incident** – the email from PowerSchool should thus say there is no evidence your SIN was involved. PowerSchool has nevertheless offered identity protection and/or credit monitoring to all individuals with any information involved. We encourage you to sign up for the services offered by PowerSchool.

When we learned of the incident, we conducted an investigation with the assistance of experts and worked diligently to request details from PowerSchool. We also worked with other school divisions in Manitoba that are similarly impacted. We have been assured by PowerSchool that the incident has been contained. We took steps to confirm there was no ongoing threat and to reduce the risk of a similar future threat, including by confirming that PowerSchool: engaged its cybersecurity response protocols, engaged a cybersecurity expert to conduct a forensic investigation, deactivated a compromised account, conducted a full password reset, initiated enhanced processes for access, further strengthened password policies and controls, and notified law enforcement. We have also informed the Manitoba Ombudsman of the incident and have attached additional information about steps you can take to help protect personal information.

Please find attached answers to some questions you may have. If you have any additional questions, they can be directed to Rob Tomlinson, Superintendent/CEO at swanvalley@svsd.ca.

In Swan Valley School Division, we take cybersecurity and protecting information seriously. We sincerely regret that this incident occurred and thank you for your continued understanding.

Regards,

Rob Tomlinson
S.V.S.D. Superintendent/CEO

[date]

Dear PowerSchool User or Parent / Guardian of User:

You are receiving this notice on behalf of [name] (the "named individual") from PowerSchool. As you may know, PowerSchool provides software and services to your current or former school or the current or former school of a person to whom you are a parent or guardian. We are writing to share with you some important information regarding a recent cybersecurity incident involving personal information belonging to the named individual.

**What Happened?**

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 our community-focused customer support portals, PowerSource.

**What Information Was Involved?**

Due to differences in customer requirements, 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, Social Insurance Number, limited medical alert information, and other related information. At this time, we do not have evidence that the named individual's Social Insurance Number was involved. At this time, we do not have evidence that limited medical alert information for the named individual was involved.

**What Are We Doing?**

PowerSchool is offering two years of complimentary identity protection services, provided by Experian, to students and educators whose information was involved. For involved students and educators who have reached the age of majority, in addition to Experian's identity protection services, PowerSchool is also offering two years of complimentary credit monitoring services provided by TransUnion.

**Offer: Experian Identity Protection Services – Available to All Involved Students and Educators**

**Enrollment Instructions for Experian IdentityWorks**

- Ensure that you **enroll by July 31, 2025** (Your code will not work after this date at 5:59 UTC)

- **Visit** the Experian IdentityWorks website to enroll: https://www.globalidworks.com/identity1
- Provide your **activation code**: MPRT987RFK
- For questions about the product or help with enrollment, please email globalidworks@experian.com

**Details Regarding Your Experian IdentityWorks Membership**

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Fraud Remediation Tips:** Self-help tips are available on your member center.

**Offer: TransUnion Credit Monitoring Services – Available to Involved Students and Educators Who have Reached the Age of Majority in their Applicable Province or Territory**

**Enrollment Instructions for TransUnion *my*TrueIdentity**

- Please visit http://www.powerschool.com/security/canada-credit-monitoring/.
- There you will find a link to the validation website, https://CACreditMonitoringValidationPage-PowerSchool.com/, where you will be prompted to validate your information by entering your first name, last name and year of birth
- If your identity is validated, a pop up will appear that provides an activation code and provides you a link to TransUnion's ***my*TrueIdentity** site to enroll
- Ensure that you enroll by May 30, 2025

**Details Regarding your myTrueIdentity Membership**

Upon completion of the online enrollment process, you will have access to the following TransUnion myTrueIdentity features:

- Unlimited online access to your TransUnion Canada credit report, updated daily. A credit report is a snapshot of your financial history and one of the primary tools leveraged for determining credit-related identity theft or fraud.

- Unlimited online access to your CreditVision® Risk credit score, updated daily. A credit score is a three-digit number calculated based on the information contained in your TransUnion Canada credit report at a particular point in time.
- Credit monitoring, which provides you with email notifications to key changes on your TransUnion Canada credit report. In today's virtual world, credit alerts are a powerful tool to help protect you against identity theft, enable quick action against potentially fraudulent activity and provide you with additional reassurance.
- Access to online educational resources concerning credit management, fraud victim assistance and identity theft prevention.
- Access to Identity Restoration agents who are available to assist you with questions about identity theft. In the unlikely event that you become a victim of fraud; a personal restoration specialist will help to resolve any identity theft. This service includes up to $1,000,000 of expense reimbursement insurance.
- Dark Web Monitoring, which monitors surface, social, deep, and dark websites for potentially exposed personal, identity and financial information and helps protect you against identity theft.

As soon as PowerSchool learned of the incident, we engaged cybersecurity response protocols and mobilized senior leadership and third-party cybersecurity experts to conduct a forensic investigation of the scope of the incident and to monitor for signs of information misuse. We are not aware at this time of any identity theft attributable to this incident.

**What Can You Do?**

You are encouraged to remain vigilant against incidents of identity theft and fraud by reviewing account statements for suspicious activity. PowerSchool will never contact you by phone or email to request your personal or account information.

**Other Important Information.**

If you have any questions or concerns about this notice, please call 833-918-7884, Monday through Friday, 8:00am through 8:00pm Central Time (excluding major US holidays). Please be prepared to provide engagement number B138905.

Sincerely,

The PowerSchool Team

## STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

### Monitor Your Accounts

**Obtain a copy of your credit report:** you may obtain a free copy of your credit report without signing up to a credit monitoring service by contacting the two Canadian credit reporting agencies:

| | |
|---|---|
| **Equifax Canada Co.**<br>National Consumer Relations<br>P.O. Box 190<br>Montreal, QC H1S 2Z2<br><br>www.consumer.equifax.ca/personal/contact-us/<br>1-800-465-7166 | **TransUnion**<br>TransUnion Consumer Relations Department<br>P.O. Box 338, LCD1<br>Hamilton, ON L8L 7W2<br><br>https://www.transunion.ca/customer-support/contact-us<br>1-800-663-9980 |

**Be cautious with communications:** remain vigilant, as always, when engaging with any unsolicited or unexpected communication, particularly those that request personal information or that refer you to a webpage that asks for your personal information, even if that communication appears to come from a source that you know and trust.

**Review your account statements and notify law enforcement of suspicious activity:** remain vigilant, as always, to the possibility of fraud and identity theft by reviewing your financial statements and accounts regularly for any unauthorized activity.

If you believe you are the victim of identity theft or fraud or have reason to believe your personal information has been misused, you should immediately:

1. **File a complaint with the police** and ask for the case reference number and the officer's name and telephone number. If you choose to obtain a copy of the police report, make sure it states your name and SIN.
2. **Contact the Canadian Anti-Fraud Centre at 1-888-495-8501** for advice and assistance about identity theft.
3. **Contact Canada's two national credit reporting agencies** to ask for a copy of your credit report. Review it for any suspicious activity. Also, check to see if your credit file should be flagged (fees may apply). To obtain additional information regarding fees and other requirements, please contact the credit reporting agencies, as described above.
4. **Inform your bank and creditors** by phone and in writing about any irregularities you identify.
5. **Report any irregularities in your mail delivery to Canada Post**, such as opened envelopes or missing financial statements or documents.
6. **Visit a Service Canada office** if you suspect that your social insurance number is being used fraudulently and bring all the necessary documents with you proving fraud or misuse. Also, bring an original identity document, such as a birth certificate or an immigration or citizenship document. An official will review your information and provide you with assistance.

**Fraud alert:** you may consider placing an alert on your credit report by contacting the two Canadian credit reporting agencies. The alert lasts six years and there may be a cost. Be prepared to supply your SIN and other basic information.

**Alert the CRA:** you can place an alert with the Canada Revenue Agency by calling 1-800-959-8281.

SWAN VALLEY
SCHOOL DIVISION

May 5, 2025

**FREQUENTLY ASKED QUESTIONS**

**The PowerSchool email and the services offered**

**1. I received an email that claims to be from PowerSchool. Is it legitimate?**

We understand PowerSchool has sent emails to students, parents/guardians, and educators whose information was involved in the incident. We understand from PowerSchool the email was or will be sent from one of the following similar email addresses: ps-sis-incident@mail.csid.com; ps-sis-incident@mail1.csid.com; or ps-sis-incident@mail2.csid.com. If you receive or have received an email from any one of these email addresses with the subject line "PowerSchool Cybersecurity Incident", we have been assured by PowerSchool that it is a legitimate email.

Whether or not you received the email from PowerSchool, you may also visit PowerSchool's website to learn how to activate the identity protection and/or credit monitoring services. The PowerSchool website also includes information in French.

**2. I have a question about how to sign up for the identity protection and/or credit monitoring services offered by PowerSchool.**

PowerSchool has advised that you can call 833-918-7884 if you have any questions.

For those able to utilize credit monitoring services (anyone age 18 and over), you will be prompted to validate before activating by entering your name and date of birth. Anyone, including those under 18, can utilize the identity protection services. We encourage you to sign up for the services offered by PowerSchool.

***The incident***

**3. What happened?**

PowerSchool informed Swan Valley School Division that it had experienced a cybersecurity incident involving unauthorized access to and exfiltration (acquisition) of certain customer information between around December 19 and December 28, 2024. Swan Valley School Division is a customer of PowerSchool, like many other educational institutions across North America. PowerSchool provides a Student Information System (SIS) used by Swan Valley School Division and thus we were informed by PowerSchool that information stored by Swan Valley School Division in our SIS was involved in the incident.

We understand PowerSchool has sent emails to students, parents/guardians, and educators whose information was involved in the incident. We understand from PowerSchool the email was or

will be sent from one of the following similar email addresses: ps-sis-incident@mail.csid.com; ps-sis-incident@mail1.csid.com; or ps-sis-incident@mail2.csid.com.

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 being offered. The PowerSchool website also includes information in French. For those able to utilize credit monitoring services (anyone age 18 and over), you will be prompted to validate before activating by entering your name and date of birth. Anyone, including those under 18, can utilize the identity protection services. 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 Swan Valley School Division as a result of this incident.

**4. Who did this and for what purpose?**

This incident occurred at PowerSchool. Unfortunately, organizations across the public and private sectors are increasingly being impacted by incidents like this.

**5. How did you respond to the incident?**

When we learned of the incident, we conducted an investigation with the assistance of experts and worked diligently to request more details from PowerSchool. We have been assured by PowerSchool that the incident has been contained. We took steps to confirm there was no ongoing threat and to reduce the risk of a similar future threat, including by confirming that PowerSchool: engaged its cybersecurity response protocols, engaged a cybersecurity expert to conduct a forensic investigation, deactivated a compromised account, conducted a full password reset, initiated enhanced processes for access, further strengthened password policies and controls, and notified law enforcement. PowerSchool has also advised that it has taken steps to prevent the information involved from further unauthorized access or misuse, that it does not anticipate the information being shared or made public, and that it believes the information has been deleted without any further replication or dissemination.

PowerSchool has notified Canadian privacy regulators about this incident. (Swan Valley School Division has already informed the Manitoba Ombudsman.) PowerSchool has or will be notifying individuals by email and we understand the email was or will be sent from one of the following similar email addresses: ps-sis-incident@mail.csid.com; ps-sis-incident@mail1.csid.com; or ps-sis-incident@mail2.csid.com. 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. The PowerSchool website also includes information in French.

For those able to utilize credit monitoring services (anyone age 18 and over), you will be prompted to validate before activating by entering your name and date of birth. Anyone, including those under 18, can utilize the identity protection services. PowerSchool has advised that you can call 833-918-7884 if you have any questions.

SWAN VALLEY
SCHOOL DIVISION

**6. 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 Swan Valley School Division as a result of this incident.

***The response***

**7. Has law enforcement been notified?**

Yes, PowerSchool has advised us that it has notified law enforcement.

**8. Has the Manitoba Ombudsman been advised?**

Yes, the Manitoba Ombudsman has been advised.

***The impact***

**9. Why did this happen to Swan Valley 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 Swan Valley School Division was a specific target in this incident.

***The data***

**10. Has information been accessed? Was information from Swan Valley School Division exposed?**

You will see that PowerSchool includes in the email a description of some of the information that was potentially involved in the incident. The information involved varies by person.

For students, the information involved will generally be limited to information parents/guardians provided Swan Valley School Division upon registration of their child as a student or any subsequent updates to that information. For many students, the information involved was name, date of birth, gender, phone number, address, school email address, doctor's name and phone number, MET number, school ID number, and/or enrolment/registration records as well as the parent/guardian's name and contact information. For a small number of students, there was also relevant medical information (e.g., allergies) and/or relevant alerts (e.g., related to discipline, guardian, custody, or other issues).

For staff, the information involved was name, date of birth, date of birth, gender, contact information, address, and/or school contact information.

The email from PowerSchool also refers to Social Insurance Number (SIN) as *potentially* involved but should also include a statement if there is no evidence that your SIN was involved – please review carefully. As we mentioned previously, based on our own investigation of the information stored in our SIS, we can advise that **no parent/guardian, staff, or student SIN, banking, or credit card information has been identified as stored in our SIS and thus was NOT involved in the incident** – the email from PowerSchool should thus say there is no evidence your SIN was involved. PowerSchool has nevertheless offered identity protection and/or credit monitoring to all individuals with any information involved. We encourage you to sign up for the services offered by PowerSchool.