LAKESHORE
SCHOOL DIVISION

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.

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 Lakeshore 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. Lakeshore School Division is a customer of PowerSchool, like many other educational institutions across North America. PowerSchool provides a Student Information System (SIS) used by Lakeshore School Division and thus we were informed by PowerSchool that information stored by Lakeshore 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. 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 Lakeshore 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. (Lakeshore 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. 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.

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 Lakeshore 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 Lakeshore 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 Lakeshore School Division was a specific target in this incident.

The data

10. **Has information been accessed? Was information from Lakeshore 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 Lakeshore School Division upon registration of their child as a student or any subsequent updates to that information. For students, the information involved was name, date of birth, gender, contact information, address, doctor's name and phone number, relevant medical information (e.g., allergies), MET number, school ID number, enrolment/registration records, and/or relevant alerts (e.g., related to discipline, guardian, custody, or other issues) as well as the parent/guardian's name and contact information.

For staff, the information involved was name, date of birth, gender, phone number, address, school email address, Professional School Personnel number, and/or school ID number.

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.

Parent/Guardians/Students

As we mentioned previously, based on our own investigation of the information stored in our SIS, **no parent/guardian or student SIN, banking, or credit card information was stored in our SIS and thus such information was NOT involved in the incident.** As such, the email from PowerSchool should 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.

Staff

As we mentioned previously, based on our own investigation of the information stored in our SIS, a subset of staff was identified as having their SIN stored in our SIS. **No staff banking, or credit card information was stored in our SIS and thus such information was NOT involved in the incident** For both staff whose SIN was stored in our SIS and for staff whose SIN was not stored in our SIS, PowerSchool has offered identity protection and/or credit monitoring to all individuals. We encourage all staff to sign up for the services offered by PowerSchool.