LAKESHORE
SCHOOL DIVISION

January 31st, 2025

Dear Lakeshore School Division Community,

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

We appreciate that more details about this incident that is impacting educational institutions across North America are needed. We have been working diligently 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.

While PowerSchool has advised that its investigation is still ongoing, it has provided some additional details and next steps:

- Identity Protection and Credit Monitoring Services: PowerSchool has engaged Experian to offer two years of complimentary identity protection services for all students and educators whose information was involved. PowerSchool has also engaged TransUnion to offer two years of complimentary credit monitoring services for all students and educators whose information was involved and who have reached the age of majority.
- Notification to Individuals Involved: Starting in the next few weeks, PowerSchool will provide notice to students, parents/guardians, and educators whose information was involved, as well as a phone number to answer any questions they may have about the incident. The notice will include the identity protection and credit monitoring services offered, as mentioned above.
- PowerSchool is in the process of notifying Canadian regulators about this incident. (Lakeshore School Division has already notified the Manitoba Ombudsman.)
- You may visit https://www.powerschool.com/security/sis-incident/ for up-to-date information on the incident.

Based on our own investigation to date of the information stored in our SIS, we can advise that while there is a subset of staff whose Social Insurance Number (SIN) were identified as stored in our SIS, no 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. With respect to the subset of individuals whose SINs were identified as *stored* in our SIS, it is not yet known if these were *involved* in the incident. **We will be contacting the staff whose SIN was identified as *stored* in our SIS out of an abundance of caution,** but these individuals will also be sent the PowerSchool notice and the identity protection and credit monitoring offers mentioned above. If any staff wish to speak further about this, please contact the Division Office.

We await additional details from PowerSchool about the findings of its investigations, the information involved in this incident, and the timing of the notices it will send. We will provide you a further update on this when available. Rest assured that when we have details to share, we are committed to sharing them.

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

In Lakeshore 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 provided below some answers to questions you may have. If you have any additional questions, they can be directed to the Division Office.

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 Lakeshore School Division that it had experienced a cybersecurity incident involving unauthorized access to certain customer information in late December 2024. Lakeshore 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 Lakeshore School Division. We await additional details from

PowerSchool about the information involved and are committing to sharing details when we have them.

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.

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, Lakeshore 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. (Lakeshore School Division has already notified the Manitoba Ombudsman.) PowerSchool has engaged Experian to offer two years of complimentary identity protection services for all students and educators whose information was involved. PowerSchool has also engaged TransUnion to offer two years of complimentary credit monitoring services for all students and educators whose information was involved and who have reached the age of majority. Starting in the next few weeks, PowerSchool will provide notice to students, parents/guardians, and educators whose information was involved, as well as a phone number to answer any questions they may have about the incident.

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 Lakeshore 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 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

9. Has information been accessed? Was information from Lakeshore School Division exposed?

PowerSchool confirmed that there was unauthorized access to certain PowerSchool customer data, including data related to Lakeshore School Division. PowerSchool's investigation is ongoing and we await additional details from PowerSchool about the

information accessed as a result of the incident. We understand that you may be looking for additional details as well. Rest assured that when we have details to share, we are committed to sharing them.

Based on our own investigation to date of the information stored in our SIS, we can advise that while there is a subset of staff whose Social Insurance Number (SIN) were identified as stored in our SIS, no 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. With respect to the subset of individuals whose SINs were identified as *stored* in our SIS, it is not yet known if these were *involved* in the incident. **We will be contacting the staff whose SIN was identified as *stored* in our SIS out of an abundance of caution,** but these individuals will also be sent the PowerSchool notice and the identity protection and credit monitoring offers mentioned above. If any staff wish to speak further about this, please contact the Division Office.