

Educating Men for Others

March 12, 2025



Dear St. Paul's High School community,

Last month, we were advised of a recent cybersecurity incident involving PowerSchool, our Student Information System (SIS) provider. Since our initial announcement to our school community (current students, parents, faculty and staff) on January 9, 2025, we have been working closely with PowerSchool to determine the specific impact on our community.

Our investigation has confirmed that for students, the accessed data includes First Name, Last Name, Date of Birth, and, if entered on the registration form, Medic Alert information. For staff, the accessed data includes First Name, Last Name, and School Email Address.

In addition, new information from PowerSchool has confirmed that alumni from the St. Paul's High School graduating classes of 2006–2024 had their information accessed in the breach, and a subset of those alumni also had their Social Insurance Numbers (SINs) accessed. This occurred because SINs were an optional field on the school's registration form during those years.

Today, we sent email notifications directly to those impacted by this data breach. However, some members of our community – including alumni from the classes of 2006 – 2024 and others who may not have received the email due to spam filtering or outdated contact information – may not have been reached. If you believe you may be affected or have any questions, please contact securityincident@stpauls.mb.ca for further assistance.

PowerSchool has assured us that, as soon as they became aware of the incident, they activated their cybersecurity response protocols and mobilized senior leadership along with third-party cybersecurity experts. A forensic investigation is ongoing to assess the scope of the breach and monitor for any signs of misuse. **Currently, PowerSchool has stated that there is no known identity theft attributable to this incident.**

PowerSchool has engaged **Experian**, a trusted credit reporting agency, to offer **two years of complimentary identity protection services** for all students and educators whose information was accessed. In addition, all adult students and educators whose information was accessed will receive **two years of complimentary credit monitoring services**, provided by **TransUnion**. To take advantage of these services, individuals must **opt in by May 30, 2025**.

PowerSchool is responsible for setting up these services, and at the time of this letter, they are still finalizing arrangements with TransUnion to ensure that all eligible individuals will be properly enrolled. We will send a follow-up notification once PowerSchool has confirmed that the process is complete. In the meantime, you may proceed with registering for the Experian Identity Protection Services as follows:

- **Experian Identity Protection Services:** Visit <https://www.globalidworks.com/identity1/> and enter the activation code: **MPRT987RFK**.
- **TransUnion Credit Monitoring Services:** Enrollment details will be provided once PowerSchool finalizes the setup.

Detailed information on this cybersecurity incident and the available Identity Protection and Credit Monitoring Services is available here:

<https://www.powerschool.com/security/sis-incident/notice-of-canada-data-breach/>

We understand that this situation may cause concern, and we remain committed to transparency as we work through this matter. If you have any questions, please do not hesitate to reach out. We appreciate your patience and trust in St. Paul's High School.

Sincerely,

A handwritten signature in black ink that reads "B. Lewin". The signature is written in a cursive, flowing style.

Bob Lewin
Principal
St. Paul's High School