Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 003-2025, 035-2025

Prairie Spirit School Division

PowerSchool Group, LLC

August 7, 2025

Summary: Prairie Spirit School Division (Prairie Spirit) contracted with PowerSchool Group, LLC (PowerSchool) to use PowerSchool's Student Information System (SIS), including PowerSchool's cloud-based SIS platform. In late 2024, a threat actor gained access to PowerSchool's systems and exfiltrated data, which included the personal information of Prairie Spirit's teachers and students. Prairie Spirit proactively reported this privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner.

The Commissioner made several findings, including that root causes of this privacy breach were: 1) the lack of employing multifactor authentication to access PowerSchool's PowerSource environment; 2) PowerSchool's failure to delete data pursuant to an agreement between Prairie Spirit and PowerSchool; and 3) Prairie Spirit's overcollection of personal information (namely students' social insurance numbers and health services numbers) increased the risk of harm in this cyber breach.

The Commissioner made several recommendations including that Prairie Spirit: 1) ensure its written agreements with information management service providers (IMSPs) meet the requirements of *The Local Authority Freedom of Information and Protection of Privacy Act* (*LA FOIP*), including section 23.2 and section 8.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* (agreements between local authority and IMSP); 2) ensure its agreements with current and future IMSPs specify the employment and enforcement of multifactor authentication; 3) conduct regular audits of its IMSPs going forward; and 4) cease the collection of social insurance numbers and health services numbers of its students and purge all remaining information of this nature from its systems; and 5) urge affected students and employees to regularly check their credit report and credit score.

Contents

I BACKGROUND

[1] PowerSchool Group, LLC (PowerSchool) provides software to schools, including a family of products called Student Information System (SIS). This system helps schools to manage and organize student data such as grades, attendance records and facilitates communications between educators, parents and students.

[2] In 2009, Prairie Spirit School Division (Prairie Spirit) began hosting PowerSchool software in its own environment. In 2015, it migrated its information to PowerSchool's cloud-based SIS platform. Also, in 2015, Prairie Spirit and PowerSchool signed a contract which was termed the "*Non-Disclosure Agreement"*. It included the following provision:

> *Data Destruction*: Upon termination of services or at any time at the request of the *PSSD* [Prairie Spirit School Division], all *PSSD* data, including any backups or copes created by *PSG* [PowerSchool], will be destroyed and formal notification of this deletion will be sent to the *PSSD* within 5 days of the request.

[3] On January 14, 2022, Prairie Spirit requested that PowerSchool cancel its subscriptions. On February 15, 2022, Prairie Spirit and PowerSchool confirmed the end dates of the subscriptions for each of the products as outlined below:

Product Name	**End Date**
PowerSchool SIS Hosting	July 11, 2022
PowerSchool SIS Hosting SSL Certificate	July 11, 2022
PowerSchool SIS Maintenance & Support	November 18, 2022
PD+ Subscription	November 18, 2022
PowerSchool SIS Customizations Maintenance & Support	January 30, 2023

[4] On January 31, 2024, Prairie Spirit contacted PowerSchool requesting that PowerSchool observe the contractual provisions in the *Non-Disclosure Agreement* and shut down the instance of SIS:

> We have discontinued our PowerSchool SIS SaaS subscription at the end of the 2021-2022 school year. At that time, we had requested the instance to be taken offline but the instance continues to still be active and able to be logged into in addition to receiving software upgrades.

> Why has this instance not been shutdown and purged as part of our discontinuing our SIS subscription? Please confirm deletion and why this instance was not removed. I can be reached by phone at [telephone number].
>
> [Emphasis added]

[5] On March 12, 2024, PowerSchool responded to Prairie Spirit indicating that the server had been decommissioned.

> Now that the server has been decommissioned it would not be possible for support to provide you with a copy of the logins as we have no way to access it. If you have any additional questions regarding it I would recommend reaching out to your customer success manager [Name and email supplied] as they may be able to put in any related requests directly to our Hosting/Cloud Ops team.

[6] Once again, on March 13, 2024, Prairie Spirit asked when the school data would be purged:

> One more question. When will the data be scrubbed from the backups as well? I want to confirm when we can expect the data to be fully purged for compliance reasons.

[7] Rather than giving a direct answer to Prairie Spirit's question, PowerSchool responded as follows on May 22, 2024:

> According to hosting your db has now been disabled. I also can not log in nor get to a url.
>
> I will move forward with closing this case by end of day on Monday but please let me know if you have any questions or concerns. I have also asked your CSM to reach out to be sure you have everything you need.

[8] Then, the following events occurred in 2024:[1]

[1] See plea agreement dated May 16, 2025 between *United States v. Matthew D. Lane* where the details in this paragraph form the basis of the information that was before the US District Court, District of Massachusetts and that was filed with the Court on May 20, 2025. The 17-year-old Mr. Matthew D. Lane pled guilty to the allegations in the information on June 6, 2025, before Judge M.R. Guzman. These facts now constitute the basis of this Investigation Report. Mr. Lane will be sentenced on September 11, 2025. Because of the plea of guilt, we now know one of the "threat actor(s)" as Matthew D. Lane. A co-conspirator remains unnamed and because the U.S.

- On or about September 4, 2024, a threat actor used the login credentials of a PowerSchool contractor to gain access to PowerSchool's computer network.
- On or about the same day, the threat actor obtained student and teacher data.
- On or about December 19, 2024, the threat actor leased a computer server from a cloud storage provider located in Ukraine.
- On or about December 20, 2024, the threat actor transferred information from PowerSchool's network to the server in Ukraine leased the day before.[2]

[9] On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving its SIS products where a threat actor exfiltrated the personal information of students, parents and educators. This information included names, dates of birth, social insurance numbers (SINs), medical information and contact information. PowerSchool received a ransom demand of 30 bitcoins. If not paid, the threat actor warranted they would leak the information "worldwide".[3] PowerSchool said the following about paying the ransom in the days following the discovery of the incident: [4]

> Any organization facing a ransomware or data extortion attack has a very difficult and considered decision to make during a cyber incident of this nature. In the days following our discovery of the December 2024 incident, we made the decision to pay a ransom because we believed it to be in the best interest of our customers and the students and communities we serve. It was a difficult decision, and one which our leadership team did not make lightly. But we thought it was the best option for preventing the data from being made public,

Department of Justice investigation is on-going, we will continue to refer to the generic "threat actor" in this matter even though one of the actors is known.

[2] PowerSchool engaged CrowdStrike Services to investigate and assess the scope and extent of the threat actor's activity in PowerSchool's environment. According to page 5 of CrowdStrike's investigation report, the earliest evidence of unauthorized activity attributable to the threat actor occurred on December 19, 2024 at 04:06:24 UTC. According to CrowdStrike Services, the threat actor exfiltrated data from PowerSchool SIS instances of PowerSchool customers between December 19, 2024 at 23:02:54 YTC and December 23, 2024 at 08:04:45 UTC.

[3] *Supra,* footnote 1, Information filed on May 20, 2025 at paragraph 14.

[4] PowerSchool Cybersecurity Incident. May 7, 2025 update. https://www.powerschool.com/security/sis-incident/.

> and we felt it was our duty to take that action. As is always the case with these situations, there was a risk that the bad actors would not delete the data they stole, despite assurances and evidence that were provided to us.

[10] On January 9, 2025, Prairie Spirit proactively reported this cybersecurity incident to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). It noted that 28,635 student records and 4,130 teacher records were impacted.[5]

[11] On January 27, 2025, PowerSchool notified OIPC of the cybersecurity incident.

[12] On April 29, 2025, OIPC notified both Prairie Spirit and PowerSchool that OIPC would be undertaking an investigation into the matter.

[13] On May 29, 2025, Prairie Spirit provided its submission to OIPC.

[14] On June 7, 2025, PowerSchool provided its submission to OIPC.

II DISCUSSION OF THE ISSUES

1. Does OIPC have jurisdiction?

[15] Prairie Spirit is a "local authority" pursuant to section 2(1)(f)(viii) of *The Local Authority Freedom of Information and Protection of Privacy Act* (*LA FOIP*).

[16] At the material time, PowerSchool was a "information management service provider" (IMSP) pursuant to section 2(1)(e.1) of *LA FOIP*.[6] Therefore, OIPC has jurisdiction and is undertaking this investigation pursuant to section 32 of *LA FOIP*.

---

[5] Prairie Spirit indicated that these numbers do not represent the true number of individuals impacted because the number of student and teacher records include original and duplicate records.

[6] PowerSchool's distinct role as an IMSP will be discussed in the analysis of whether a privacy breach occurred.

2. Did a privacy breach occur?

[17] A privacy breach occurs when personal information is collected, used and/or disclosed in a way that is not authorized by *LA FOIP*. The first step in determining if a privacy breach has occurred is to identify if personal information is involved in this matter. If so, the second step is to determine if the personal information was collected, used and/or disclosed in a way that was not authorized by *LA FOIP*.

a. Is personal information involved in this matter?

[18] Personal information is defined by means of a long list in section 23(1) of *LA FOIP*, though the list is not exhaustive. Personal information is information that is about an identifiable individual, and that is personal in nature. Information is about an identifiable individual if the individual can be identified from the information; examples include a person's name or social insurance number. Further, information is personal in nature if it provides something identifiable about the individual.[7]

[19] Within PowerSchool's SIS were two tables (the student table and teacher table) from which the threat actor exfiltrated data. Prairie Spirit provided OIPC with samples of the student table and the teacher table. The student table contained information such as:

- Student's name,
- Student identification number,
- Enrollment status,
- Grade level,
- Gender,
- Entry date,
- Exit date,
- WEB ID,
- WEB Password,
- School identification number,
- Date of birth,
- Address,
- SIN

[7] See OIPC Investigation Report 253-2024, 033-2025 at paragraph [14].

- Name of doctor,
- Doctor's phone number,
- Name of mother
- Mother's phone number
- Name of father
- Father's phone number,
- Year of graduation, and
- Medical information, such as health services number (HSN).

[20] The teacher table contained information such as:

- Teacher's name,
- Title (e.g. Ms., Mrs., Mr. etc.)
- Password,
- Teacher number,
- SIN
- Home phone number, and
- Mailing address.

[21] Upon review, most of the fields listed above qualify as "personal information" as defined by sections 23(1)(b), (c), (d), (e) and (k)(i) of *LA FOIP* as follows:[8]

> **23**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> …
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> (c) information that relates to health care that has been received by the individual or to the health history of the individual;
>
> (d) any identifying number, symbol or other particular assigned to the individual;
>
> (e) the home or business address, home or business telephone number, fingerprints or blood type of the individual;

[8] See OIPC Review Report 031-2020 at paragraphs [6] and [7]; OIPC Review Report 286-2023 at paragraph [149].

> ...
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual;

[22] There will be a finding that the information involved in this matter qualifies as personal information as defined by sections 23(1)(b), (c), (d), (e) and (k)(i) of *LA FOIP*.

b. Was the personal information collected, used and/or disclosed without authority under *LA FOIP*?

[23] Prairie Spirit signed a *Non-Disclosure Agreement* with PowerSchool in October 2015 that outlined how PowerSchool would manage data on behalf of Prairie Spirit. As such, PowerSchool qualifies as an IMSP for Prairie Spirit pursuant to section 2(1)(e.1) of *LA FOIP*:

> **2**(1) In this Act:
>
> ...
> (e.1) **"information management service provider"** means a person who or body that:
>
> (i) processes, stores, archives or destroys records of a local authority containing personal information; or
>
> (ii) provides information management or information technology services to a local authority with respect to records of the local authority containing personal information;

[24] To have "control" over a record means that a local authority has authority over any personal information involved. This includes the authority to manage the record including restricting, regulating, and administering its use, disclosure or disposition.[9] So, while Prairie Spirit's data was on PowerSchool's system, the information always remained within Prairie Spirit's care and control. Prairie Spirit always retained the paramountcy over this information and still had to honour the duty of protecting it.

[9] See OIPC Investigation Report 035-2024, 047-2024, 052-2024, 059-2024 at paragraph [17].

[25] *LA FOIP* does not define the terms "collection", "disclosure" or "exfiltration", however this office offers these definitions:[10]

- "Collection" means the bring or come together, assemble, accumulate, obtain personal information from any source by any means;

- "Disclosure" is the sharing of personal information with a separate entity, not a division or branch of the local authority in possession or control of that information.

- "Exfiltration" means, in this case, to steal sensitive data from a computer.

i. What constitutes an exfiltration of data within a privacy breach?

[26] Based on the above definitions, the exfiltration of personal information constitutes an unwarranted "disclosure" of personal information. In this case, the threat actor exfiltrated the personal information from Prairie Spirit for its own illegal purposes – yet this was a disclosure of the personal information because the information was always under the care and control of Prairie Spirit. Section 28 of *LA FOIP* prohibits local authorities such as Prairie Spirit from disclosing personal information unless the local authority has consent of the holder of the personal information, or if the disclosure is authorized pursuant to sections 28(2) or 29 of *LA FOIP*. In this case neither section 28(2) or section 29 are relevant to this set of facts. The disclosure of the personal information to the threat actor in this matter was not permitted according to *LA FOIP*. Therefore, there is a finding that a privacy breach occurred when the threat actor exfiltrated the personal information that was in the care and control of Prairie Spirit.

ii. The overcollection of personal information by Prairie Spirit and the resulting risk

[10] See OIPC Investigation Report 279-2024 paragraph [25] to [27]. The definition of "exfiltration" is from Merriam-Webster online.

[27] In a review of the exfiltrated personal information, Prairie Spirit collected the SINs and/or HSNs of some of its students. Section 24 of *LA FOIP* provides as follows:

> **24** No local authority shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the local authority.

[28] Prairie Spirit indicated that the SINs of some students were collected and stored in PowerSchool SIS. This office sought an explanation from Prairie Spirit as to why schools would need to collect student SINs. Prairie Spirit could not be sure and speculated that some schools may have collected SINs in PowerSchool as part of students participating in work placement. The Office of the Privacy Commissioner of Canada (OPC) has advised that individuals should provide a SIN *only* when legally required and in very limited circumstances related to personal finances: such as to obtain payment for employment purposes, to open financial accounts or to receive certain government services or payments.

[29] Similarly, the HSNs of some students were also collected and stored in the PowerSchool SIS. This office has explained why it is not advisable that schools require such information from students:[11]

> An individual's HSN is considered their personal health information and under HIPA also provides that an individual is not required to provide their HSN unless they are receiving a health care service or otherwise where required by another Act or regulation. An individual's personal health information is considered more sensitive than other personal information and HIPA provides that personal health information shall be collected on a need-to-know basis. Does your child's school have a need-to-know your child's personal health information?
>
> You may think that the school is requesting your child's HSN in the event that your child is injured at school and requires a trip to the doctor's office or hospital, the parent or guardian will be called to pick up the child or meet the child at the health care facility. Chances are, in an emergency, the school will

[11] Section 11 of *The Health Information Protection Act* (HIPA) speaks to individuals' right to refuse to produce their HSN to any person (other than a trustee who is providing a health service) as a condition of receiving purpose. Further, it provides that no person shall require an individual to produce their HSN as a condition of receiving any product or service. See also this OIPC blog post: Should you provide your child's HSN to their school? | IPC

> not be searching through their records to find the child's HSN. The health care facility will not refuse to treat your child and will collect personal information from the parent or guardian once you arrive at the facility. In another scenario, your child may be offered an immunization at school, but this service is not offered by the school and will be offered by a trustee. You also have the right to consent each time a health service might be offered to your child. If you consent to the service, the trustee has a need to know and your child's HSN can be collected by the trustee at that time.

[30] Similarly, a committee that includes the Saskatchewan School Boards Association (SSBA) has publicly advised the following:[12]

> School divisions do not need to have student HSN for emergency situations. If a student is injured and must be taken to a doctor or a hospital, the student will be treated even if the student does not have a HSN with them at the times.

[31] Further, the SSBA warns on its website:[13]

> There is no instance in which the HSN should be routinely collected on school division registration forms.

[32] A privacy breach, in its own right, occurs every time there is an overcollection of personal information. Clearly, the threat actor – a cyber criminal was responsible for the primary privacy breach in this case. Nevertheless, the overcollection of SINs and HSNs on the part of Prairie Spirit aggravated the extent of the exfiltration of personal information in the privacy breach. We are now left with a compounded overall risk to the affected individuals in this province. OIPC will comment on this risk and suggest helpful recommendations later in this Investigation Report.

---

[12] Privacy and Access in Saskatchewan Schools. *Disclosure of Saskatchewan Health Numbers*: https://saskschoolsprivacy.com/central-adminstration/student-records/use-access-disclosure-of-student-records/disclosure-of-saskatchewan-health-numbers/. The committee is made up of the Saskatchewan School Boards Association, Saskatchewan Teachers' Federation, Saskatchewan Ministry of Education, League of Educational Administrators, Directors and Superintendents of Saskatchewan and Saskatchewan Association of School Business officials. For more information, see the About webpage of Privacy and Access and Saskatchewan Schools.

[13] Privacy and Access in Saskatchewan Schools. *Disclosure of Saskatchewan Health Numbers*: https://saskschoolsprivacy.com/central-adminstration/student-records/use-access-disclosure-of-student-records/disclosure-of-saskatchewan-health-numbers/.

3. Did Prairie Spirit respond to the privacy breaches appropriately?

[33] The analysis of a local authority's response to a privacy breach involves several factors. Whether a local authority appropriately responds to a privacy breach and takes proper corrective measures is informed by section 6-7 of OIPC's *Rules of Procedure*. The considerations include:

(a) Was the breach contained;

(b) Were the affected individuals notified;

(c) Was the breach investigated; and

(d) Were appropriate steps taken to prevent future breaches.

a. Containment of the Breach

[34] Upon learning that a privacy breach has occurred, local authorities should take immediate steps to contain the breach. Depending on the nature of the breach, this can include: [14]

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; and
- Correcting weaknesses in physical security.

[35] As detailed in the factual recitation of this Investigation Report, Prairie Spirit cancelled its subscription with PowerSchool on January 14, 2022 and an agreement was reached with respect to the termination dates for each of the subscriptions as outlined in paragraph [3] of this Investigation Report. By January 31, 2024, Prairie Spirit noted that the terminations still had not been effected so it wrote PowerSchool and asked why the instance of SIS was

[14] See Investigation Report 211-2024 at paragraph [19]; See also OIPC's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

not terminated and all data not purged. Prairie Spirit specifically requested the purging of its data once again on March 13, 2024, but a firm confirmation from PowerSchool that the data was indeed purged did not follow. Instead, Prairie Spirit was content with the May 22, 2024 notification from PowerSchool that the database had been "disabled".

[36] Confirmation that PowerSchool had purged the Prairie Spirit data was crucial and should have been pursued by Prairie Spirit, because had the data been properly purged, this privacy breach would not have affected any individuals in Saskatchewan.

[37] Upon being made aware of the cyberbreach, we now know PowerSchool took the following essential containment steps: [15]

- Deactivated the compromised credential.
- Enforced a full password reset for employees and contractors.
- Restricted access to and tightened password and access controls for the affected customer support portal.
- Required that access to the PowerSource environment be via the company's Virtual Private Network (VPN), which required single sign-on and multi-factor authentication. [16]

[38] Further, as noted in the factual recitation of this Investigation Report, PowerSchool paid a ransom fee to the threat actor despite the risk that the stolen data could never be confirmed as purged. [17] Sadly, in circumstances such as this, there can be no guarantee of containment.

[39] This office notes the commitment on the part of the Privacy Commissioner of Canada, Mr. Philippe Dufresne, to monitor the PowerSchool's commitments to the victims of the

[15] See page 3 of the CrowdStrike's investigation report which outlined the steps taken by PowerSchool, dated February 28, 2025.

[16] PowerSource is customer support portal for PowerSchool products.

[17] PowerSchool Cybersecurity Incident. May 7, 2025 update at https://www.powerschool.com/security/sis-incident/.

Canadian privacy breach. Considering the actions that PowerSchool has already implemented, and the actions to be taken in the coming months, the Privacy Commissioner of Canada has agreed to discontinue his February 2025 investigation into the PowerSchool cyberbreach across Canada. Since this is an ongoing matter, this office will refrain from comment on the reasonableness of the actions taken by PowerSchool to contain this breach but we note the following public statement by the federal Privacy Commissioner with respect to PowerSchool's actions in response to the breach: [18]

> PowerSchool took measures to contain the breach, notify affected individuals and organizations and offer credit protection, and has voluntarily committed to additional actions to support its security safeguards. These include strengthened monitoring and detection tools.

b. Notification of Affected Individuals

[40] Section 28.1 of *LA FOIP* requires local authorities to take all reasonable steps to notify affected individuals when it is believed the privacy breach creates a real risk of significant harm to the affected individuals:

> **28.1** A local authority shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[41] Whether there is a real risk of significant harm or not, it is best practice for local authorities to inform affected individuals when their personal information has been involved in a privacy breach. The local authority must also identify possible risks to the affected individuals and inform them of steps they can take to protect themselves. [19]

[18] See Privacy Commissioner of Canada News Release July 22, 2025: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2025/nr-c-20250722/

[19] See Investigation Report 211-2024 at paragraph [25]; See also OIPC's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[42] The information a local authority should include in a notice to affected individuals may include:[20]

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.).
- A description of possible types of harm that may come to the affected individual because of the privacy breach.
- Steps taken and planned to mitigate the harm and prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies).
- Contact information of an individual within the organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to OIPC (provide OIPC's contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

[43] Soon after learning about the PowerSchool cybersecurity breach, Prairie Spirit sent letters to all families and staff at the school to provide general information about the incident. The letters, dated January 10, 2025 and January 28, 2025, included brief descriptions of what personal information was involved and what PowerSchool was doing in response.

[44] Prairie Spirit then sent a letter dated February 14, 2025 to the individuals directly impacted by the cybersecurity breach. That letter contained all the necessary elements to make for an effective notice, including information on how individuals can sign up for two years of credit monitoring that was being offered by PowerSchool.

[45] On February 25, 2025, Prairie Spirit also emailed former students and/or contacts a link to a form that could be completed to determine if their personal information was impacted by

[20] See Investigation Report 253-2024, 033-2025 at paragraph [36].

the cybersecurity breach. After submitting the form, individuals would receive a personalized email from Prairie Spirit of the results.

[46] Prairie Spirit further contacted the Ministry of Education to obtain the contact information of individuals for whom the school division no longer had up-to-date contact information. On February 26, 2025, Prairie Spirit sent an email to those individuals. The email had a link to Prairie Spirit's February 14, 2025 letter that provided notice of the cybersecurity breach.

[47] On March 7, 2025, Prairie Spirit posted a message to the general public on its website and its social media channels to notify anyone that may have been missed in its previous messages. The message board was important because it was in bold white and letter type against a dark blue background and it offered a link for affected individuals to immediately confirm whether or not their information had been impacted by the breach:

> We have attempted to notify all known individuals affected by the PowerSchool cybersecurity incident discovered on December 28, 2024.
>
> If you attended a Prairie Spirit school or worked at Prairie Spirit between 2009 and 2022 and have not been contacted, please use the link in this post to check if your information was impacted.

[48] On May 9, 2025, and for the month of June 2025, Prairie Spirit posted an update message board to its website. This message was crucial because it notified affected individuals that there was some concern with respect to the possible misuse of the breached data, but it assured the community that this was not a new breach. The message board provided a link to further details and support on the PowerSchool website:

> Message for Prairie Spirit families
>
> PowerSchool cybersecurity incident
>
> We want to inform our community about a recent update regarding the PowerSchool cybersecurity incident form December 2024. PowerSchool has shared that a threat actor may be attempting to misuse data from the original incident. This is not believed to be a new breach.

> PowerSchool continues to offer two years of credit monitoring and identity protection services to affected students and staff.

[49] Based on the above, there will be a finding that Prairie Spirit made reasonable efforts to notify affected individuals of this privacy breach in a timely and best practices fashion.

c. Investigation of the Breach

[50] Once containment has been addressed and appropriate notification given, the local authority should investigate. The investigation must address the incident on a systemic basis and include a root cause analysis and conclusion. The local authority must consider its duty to protect personal information as set out at section 23.1 of *LA FOIP*. Specifically, section 23.1 of *LA FOIP* requires that local authorities establish policies and procedures to maintain administrative, technical and physical safeguards:

> **23**.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[51] In assessing the root cause of a privacy breach, the local authority must formulate safeguards that would have prevented the privacy breach from occurring in the first place.[21]

[21] See OIPC Investigation Report 003-2025, 035-2025 at paragraph [41].

i. The need for multifactor authentication

[52] The threat actor obtained compromised login credentials and was able to gain access to PowerSchool's PowerSource environment because of an essential vulnerability in the security of PowerSchool's systems – the lack of multifactor authentication. Even with compromised login credentials, multifactor authentication could have prevented the threat actor from gaining access because the second phase of the verification process would have been impossible. There will be a finding that a root cause of this privacy breach was the lack of employing multifactor authentication.[22]

ii. PowerSchool's failure to purge

[53] Another obvious root cause of this privacy breach was PowerSchool's failure to delete and purge the data pursuant to the *Non-Disclosure Agreement* with Prairie Spirit - despite the school's repeated demands. Similarly, Prairie Spirit should have considered immediate legal action to ensure that the data was purged upon termination of the contract and pursuant to the contractual agreement it had with PowerSchool and the dates that were presented for the end dates of the subscriptions as outlined in paragraph [3] of this Investigation Report. The assurance it got from PowerSchool as late as May 2024 was only with respect to the disabling of the database. We now know that the breach occurred in September of 2024. Prairie Spirit fell short of its obligations to protect the personal information of its students and faculty.

[54] Some months after the cyberbreach, Prairie Spirit followed up with PowerSchool on February 18, 2025 requesting confirmation that its (Prairie Spirit) data "is not still stored" on PowerSchool's server.

[22] *Supra,* footnote 2 at page 3 – the Background summary includes four steps taken by PowerSchool to prevent data from further unauthorized access or misuse. The implementation of multifactor authentication is crucial to this set of facts.

[55] On February 26, 2025, PowerSchool issued a certificate of destruction to Prairie Spirit.

[56] On March 28, 2025, PowerSchool admitted to Prairie Spirit that the decommissioning process took too long:

> …as concerns your question about the decommission process, you are correct that the full decommission process was not completed immediately after the exchange in February 2022. PowerSchool acknowledges the full process did not get completed until your receipt of the signed Certificate of Data Destruction. A full decommission process would never be completed in one day or in most cases within a few months. This is because permanent data deletion also requires that we ensure back-ups of data no longer contain the decommissioning customer's data. Nevertheless, this duration of full decommission for Prairie Spirit School Division was too long. We sincerely apologize for that and appreciate your understanding and trust that with your receipt of the signed Certificate of Data Destruction in hand, you can now be confident that the process is completed.

[57] PowerSchool's admission that its decommissioning process took too long is a crucial concession. Had PowerSchool fulfilled its contractual obligations, students and employees of Prairie Spirit would have been immune to this privacy breach.

iii. The Non-Disclosure Agreement did not recognize *LA FOIP*

[58] The *Non-Disclosure Agreement* addressed the management of the PowerSchool data. The contract represented that the confidentiality of the data would be preserved, and it prohibited PowerSchool from selling, marketing, or mining the data. However, OIPC noted that the agreement omits a crucial reference. It does not cite the guiding law in Saskatchewan - *LA FOIP*. Rather, it referenced the federal "*Canadian Privacy Act*":

> In consideration of the mutual covenants of this *Agreement*, [PSG - PowerSchool Group, LLC] agrees to abide by the privacy regulations of both the *Canadian Privacy Act* and the *Privacy and Access in Saskatchewan Schools* provincial policy in conjunction with the following terms and conditions of access, disclosure and retention.

[59] Prairie Spirit is subject to the provisions of *LA FOIP*, and this statute is not a "provincial policy". It is also important to note that Prairie Spirit is not subject to the jurisdiction of the

federal *Privacy Act* because that federal statute protects the privacy of individuals with respect to personal information about themselves held by a federal government institution.[23] The citing of the incorrect legislation lends to an inference that Prairie Spirit was not familiar with the requirements of *LA FOIP* and that it failed to ensure that the *Non-Disclosure Agreement* met the requirements of the proper provincial law. There will be a finding that Prairie Spirit failed to ensure the agreement met the requirements of *LA FOIP* when it entered into a contractual agreement with PowerSchool as its IMSP.

[60] Prairie Spirit must ensure its contractual agreements with future IMSPs meet the requirements of *LA FOIP* and *The Local Authority Freedom of Information and Protection of Privacy Regulations* (*LA FOIP Regulations*). Section 23.2(2) of *LA FOIP* sets out specific requirements that must be in an information sharing agreement between a local authority and an IMSP that will protect both the local authority and the individuals the local authority acts on behalf of:

> **23.2**(2) Before disclosing personal information to an information management service provider, the local authority shall enter into a written agreement with the information management service provider that:
>
> (a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the personal information;
>
> (b) provides for the protection of the personal information; and
>
> (c) meets the requirements of this Act and the regulations.

[61] *LA FOIP* was amended in 2017 to include section 23.2. That same year the *LA FOIP Regulations* were amended to include section 8.2. Prairie Spirit should have kept abreast of the law and amended its *Non-Disclosure Agreement* in 2017 to reflect these requirements because section 8.2(c) of the *LA FOIP Regulations* provides specifically for the purging of data:

> **8.2** For the purposes of clause 23.2(2)(c) of the Act, a written agreement that is entered into between a local authority and an information management service provider must include:

[23] *Privacy Act,* RSC 1985, c.P-21, as amended.

> (a) a description of the specific service the information management service provider will deliver;
>
> (b) provisions setting out the obligations of the information management service provider respecting the security and safeguarding of personal information; and
>
> (c) provisions for the destruction of the personal information, if applicable.

[62] The provisions of section 23.2(2) of *LA FOIP* and section 8.2 of the *LA FOIP Regulations*, required that Prairie Spirit effect due diligence prior to the assumption of a contractual agreement with an IMSP. Prairie Spirit should have taken measures to identify potential risks and appropriate safeguards with respect to the contracting of an IMSP. Many bodies contract out with knowledgeable sources to perform this essential duty, but it is important to have in place to mitigate such risks. With this in mind, the completion of a security threat risk assessment is always recommended.[24]

[63] A specific provision mandating a fine or return of moneys in the event of failure to purge would have been useful leverage for Prairie Spirit to engage a faster response to its request for the wiping of its data.

iv. Failure to audit

[64] The *Non-Disclosure Agreement* provided Prairie Spirit with the right to audit PowerSchool's data transferal practices. The agreement provided:

> The PSSD has the right to audit and inspect the vendor's practices with respect to data transferred. An SOC-2 or similar may be requested not more frequently than once per school year. The Parties agree to work together to determine a reasonable time and place for said inspection.

[24] To learn more about the process involved for security threat risk assessments, see the following page supplied by the Government of British Columbia: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-threat-and-risk-assessment

[65] This is an important provision within the *Non-Disclosure Agreement* since it gave Prairie Spirit the ability to ensure PowerSchool was managing personal information in compliance with *LA FOIP* – had *LA FOIP* been correctly identified as the governing statute.

[66] Prairie Spirit conceded that it failed to conduct any audits or inspections of PowerSchool. However, it noted that PowerSchool's System and Organization controls (SOC) 2 reports were available through PowerSchool's support site. Prairie Spirit indicated that it did not have concerns resulting from the findings of the SOC 2 reports.[25]

[67] While it is good practice to ensure IMSPs are compliant with auditing standards, this privacy breach reveals that compliance with such standards cannot remove the need for continually identifying security risks and implementing methods to mitigate such risks. Going forward, Prairie Spirit should regularly engage in an audit of its IMSPs to ensure that they comply with the provisions of their contractual agreements and that those agreements have been drafted in accordance with *LA FOIP*.

v. Overcollection of personal information

[68] Prairie Spirit engaged in the overcollection of personal information, namely the SIN and HSN of its students. We cannot leave this Investigation Report without a comment on the dire consequences of the overcollection of personal information.

[69] The loss of a SIN leaves individuals vulnerable to serious fraud and identity theft.

[70] The loss of a HSN leaves an individual vulnerable to medical identity theft. Medical identity theft occurs when individuals, other than the person assigned to the HSN, obtain medical services. Not only is this a fraud upon the state, but it can lead to inaccuracies in

[25] According to Business Development Bank of Canada (BDC), the SOC 2 (Systems and Organization Controls 2) is a compliance and privacy standard used in North America that uses an auditing framework to monitor not just the integrity of data in the financial sector but data in the cloud. This cybersecurity compliance standard specifies ways for organizations to ensure their data is stored and processed securely.

the victim's health profile and it can affect the health services an individual may receive in the future.

[71] There is no need for a school to collect SINs and HSNs from its students. There will be a recommendation that Prairie Spirit cease to collect this information. There is also a recommendation that Prairie Spirit review its current records and purge any past and present records of student SIN and HSNs held either by the school or its current IMSPs.

[72] PowerSchool offered two years of credit monitoring to affected individuals. This is an appropriate and commendable offer of service. There will also be a recommendation that Prairie Spirit urge affected students and employees to regularly monitor their credit report and credit score. The government of Canada provides a useful link to assist with this activity. [26] Credit monitoring is a key indicator of problems linked to identity theft. As we have noted, there is no guarantee of containment of data in cyberbreaches of this nature. That is, the data may very well have been sold to criminals on the Dark Web who may use it *at any time in the future*. Affected individuals must be reminded to be vigilant in their efforts to protect themselves against fraud and identity theft.

d. Prevention of Future Breaches

[73] It is crucial to ensure the implementation of measures to prevent similar breaches from occurring in the future. Possible prevention measures may include adding/enhancing safeguards already in place, the provision of additional training, and the regular monitoring/auditing of systems and system users. The following considerations are relevant: [27]

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?

[26] Getting your credit report and credit score - Canada.ca

[27] See OIPC Investigation Report 253-2024, 033-2025 at paragraph [50]; See also OIPC's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

- Is additional training needed?
- Should a practice be stopped?

[74] Prairie Spirit no longer contracts with PowerSchool SIS nor uses its products. Therefore, we now focus on Prairie Spirit's contractual agreements with current and future IMSPs. To begin with, Prairie Spirit should ensure that all present and future agreements with an IMSP acknowledge and stipulate the requirements of *LA FOIP* and the *LA FOIP Regulations*.

[75] We commend Prairie Spirit in its efforts to engage two of its current IMSPs regarding their data destruction processes. We note that Prairie Spirit now requires certificates of destruction and/or confirmation that data has been purged upon request.

[76] There will be a finding that Prairie Spirit is taking reasonable steps to prevent a similar privacy breach in the future.

4. Concluding Words

[77] This situation highlights the need for public bodies to understand that their obligations and duties with respect to the personal information of those in its care cannot be contracted out absolving the public body of all responsibilities. The need to manage and protect the data is always under the control of a public body even when a contract with a IMSP has been engaged. To this end, it is essential that public bodies must always negotiate the terms of the contractual agreement to which they outsource the protection of the personal information and ensure that the proper provincial statute, *LA FOIP*, is the designated legal authority. Public bodies must be prepared to understand the application of the proper legislation, in this case *LA FOIP*, and they must be prepared to regularly audit and ensure that the IMSP abides by the terms of the agreement. If there is non-compliance, the public body must be prepared to seek immediate compliance by legal means. A contract with an IMSP does not mean that the original collector of the information is relieved of all responsibility for the integrity of the data. Flowing from this, there will be a recommendation that Prairie Spirit ensure that its current and future contracts with an IMSP

meet the requirements of *LA FOIP* and the *LA FOIP Regulations* and require multifactor authentication to access the data.

III FINDINGS

[78] OIPC has jurisdiction to undertake this investigation.

[79] The information in question in this Investigation Report qualifies as personal information as defined by sections 23(1)(b), (c), (d), (e) and (k)(i) of *LA FOIP*.

[80] A privacy breach occurred when the threat actor exfiltrated the personal information of Prairie Spirit.

[81] The overcollection of personal information on the part of Prairie Spirit increased the risk of harm for the affected victims in this privacy breach.

[82] Prairie Spirit made reasonable efforts to notify affected individuals of this privacy breach in a timely and best practices fashion.

[83] A root cause of this privacy breach was the failure of PowerSchool to initiate a multifactor authentication process prior to the accessing of the PowerSource environment.

[84] A root cause of this privacy breach was PowerSchool's failure to delete data pursuant to the contractual terms of the *Non-Disclosure Agreement* with Prairie Spirit.

[85] The *Non-Disclosure Agreement* between Prairie Spirit and PowerSchool did not acknowledge and stipulate the requirements of *LA FOIP*.

[86] Prairie Spirit failed to engage in a regular audit of PowerSchool to ensure compliance with the provisions of their contractual agreement and those of *LA FOIP*.

IV RECOMMENDATIONS

[87] I recommend that Prairie Spirit ensure its current and future written agreements with IMSPs meet the requirements of *LA FOIP* and the *LA FOIP Regulations*, including section 23.2(2) of *LA FOIP* and section 8.2 of the *LA FOIP Regulations*.

[88] I recommend that Prairie Spirit ensure its agreements with current and future IMSPs specify the employment of multifactor authentication.

[89] I recommend the immediate cessation of overcollection of personal information, in particular the collection of student SIN and HSN on the part of Prairie Spirit.

[90] I recommend that Prairie Spirit review and purge its current records, and that of a current IMSP, of student SINs and HSNs.

[91] I recommend that Prairie Spirit urge affected students and employees to regularly check their credit report and credit score.

Dated at Regina, in the Province of Saskatchewan, this 7th day of August, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner