Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 129-2024

Ministry of Advanced Education

December 16, 2024

Summary: The Ministry of Advanced Education (Advanced Education) proactively reported a privacy breach to the Commissioner's office after it mailed "Statement of Pension, Retirement, Annuity, and Other Income" forms relating to student grants to the wrong addresses. The A/Commissioner investigated the incident under *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*. He found that there was a privacy breach involving personal information and personal health information. He found that Advanced Education took appropriate action to contain and investigate the breach. He also found that Advanced Education took appropriate steps to prevent further breaches of this kind. However, the A/Commissioner found that Advanced Education's notification to affected parties was not adequate. The A/Commissioner recommended that Advanced Education, within 30 days of the issuance of this Investigation Report, send a letter to the affected parties offering credit monitoring services to them for one year. He also recommended that Advanced Education, within 30 days of the issuance of this Investigation Report, amend its template for future breach notifications to include information about the risks that may arise from a breach and how to address those risks.

I BACKGROUND

[1] This Investigation Report considers a privacy breach that was proactively reported to my office on May 6, 2024, by the Ministry of Advanced Education (Advanced Education).

[2] Advanced Education reported that a breach occurred on February 15, 2024, when it mailed 415 "Statement of Pension, Retirement, Annuity, and Other Income" forms (T4A slips) to the wrong individuals. The employee responsible for producing the mailing labels made a

mistake when working with an Excel spreadsheet that was used to print the labels that resulted in the incorrect address appearing on the labels.

[3] Advanced Education reported that the breach affected 277 individuals. The number of affected individuals was less than the number of misdirected T4A slips because some individuals received more than one T4A slip.

[4] An affected individual contacted our office regarding their concerns about the risk of identity theft. Four other individuals asked my office to notify them of the results of my office's investigation.

[5] On May 16, 2024, my office notified Advanced Education that my office would be conducting an investigation into the privacy breach. On June 19, 2024, Advanced Education provided my office with its completed *Privacy Breach Investigation Questionnaire* (Questionnaire).

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] Advanced Education qualifies as a "government institution" pursuant to subsection 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP).

[7] As set out in my office's *Guide to FOIP*, Chapter 6, "Protection of Privacy", updated February 27, 2023 (*Guide to FOIP*, Ch. 6) at page 32, the privacy rules in FOIP only apply to personal information. Therefore, I must determine if the information at issue qualifies as personal information under subsection 24(1) of FOIP.

[8] Advanced Education stated that it mailed the T4A slips to individuals receiving grants under the "Canada Grant for Services and Equipment for Students with Disabilities" program. According to information publicly available on the Saskatchewan government

website, these grants are, generally speaking, for students who have financial need, a disability and the need for education-related services or equipment.

[9] The misdirected T4A slips contained information such as the names of the individuals receiving grants, their social insurance number and the amounts received during the calendar year.

[10] Individuals' names would qualify as their personal information because they appear with other information about them (subsection 24(1)(k) of FOIP). Individuals' social insurance numbers would qualify as personal information pursuant to subsections 24(1)(d) of FOIP because they are an identifying number assigned to the individuals. The information about the amounts paid on the T4A slip would qualify as personal information pursuant to subsection 24(1)(b) of FOIP because it is information about financial transactions relating to them. Information on the T4A slips about grants to students with disabilities would reveal that the student had a disability. If this information was on a T4A slip it would qualify as a student's personal information pursuant to subsection 24(1)(a) of FOIP.

[11] These subsections of FOIP provide as follows:

> **24**(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:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> (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;
>
> …
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
>
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or

[12] Accordingly, I find that the information at issue qualifies as personal information pursuant to subsections 24(1)(a), (b), (d) and (k) of FOIP and the privacy rules set out in Part IV of FOIP apply to this breach.

[13] Given the inclusion of information that would reveal an individual's disability, I must also consider if *The Health Information Protection Act* (HIPA) applies to this incident. HIPA is only engaged if three elements exist: (1) there is a trustee within the meaning of subsection 2(1)(t) of HIPA; (2) there is personal health information involved within the meaning of subsection 2(1)(m) of HIPA; and (3) the personal health information is in the custody and control of the trustee at the time of the incident.

[14] Advanced Education qualifies as a trustee under subsection 2(1)(t)(i) of HIPA which states:

> **2**(1) In this Act:
>
> …
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> (i) a government institution;

[15] As to whether personal health information is involved, Advanced Education stated that some of the T4 slips might include information that would reveal that the individual had a disability. Previous reports of my office, including Investigation Report 113-2020, have found that information about a person's disability qualifies as their personal health information. Therefore, information in the T4A slip that would reveal that an individual has a disability qualifies as their personal health information pursuant to subsection 2(1)(m)(i) of HIPA which states:

> **2**(1) In this Act:
>
> …
> (m) "personal health information" means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;

[16] Finally, as the information about an individual's disability is contained in the record holdings of Advanced Education, it has custody or control of the information. All three elements are present for HIPA to be engaged.

[17] Therefore, I find that I have jurisdiction to conduct this investigation pursuant to both FOIP and HIPA.

2. Did Advanced Education respond appropriately to the privacy breach?

[18] Advanced Education acknowledged that a privacy breach occurred. It also acknowledged that the information at issue involved personal information and personal health information. Advanced Education does not appear to have considered how HIPA applied to this breach even though it acknowledged that the information included personal health information.

[19] In circumstances where there is no dispute that a privacy breach has occurred, my office's investigation focuses on whether the government institution or trustee has appropriately handled the breach.

[20] As set out in sections 4-4 (applies to FOIP) and 5-4 (applies to HIPA) of my office's *Rules of Procedure* and my office's *Guide to FOIP*, Ch. 6 at page 273, and my office's *Privacy Breach Guidelines for Trustees*, at pages 3 to 6, my analysis of Advanced Education's responses to the privacy breach looks at its efforts to:

1. Contain the breach (as soon as possible);
2. Notify affected individuals (as soon as possible);
3. Investigate the breach; and
4. Prevent future breaches.

[21] I turn to consider if Advanced Education appropriately addressed each of these steps.

Contain the breach (as soon as possible)

[22] My office's *Guide to FOIP*, Ch. 6 at page 273 and *Privacy Breach Guidelines for Trustees* at page 3, state that upon learning that a privacy breach has occurred, government institutions and trustees should immediately take steps to contain the breach. Depending on the nature of the breach, this may include:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that has been breached.
- Revoking accesses to personal information.
- Correcting weaknesses in physical security.

[23] In my office's Investigation Report 197-2022, 215-2022, I stated that in assessing efforts to contain the breach, my office applies a reasonableness standard. We want to have some reassurance that the institution or trustee has reduced the magnitude of the breach and the risk to affected individuals.

[24] The following timeline of key events is based on information provided by Advanced Education:

- February 15, 2024 – Advanced Education mailed 415 T4A slips relating to 277 students to the wrong addresses.
- February 19, 2024 – Advanced Education learned of the breach when two students called its office to report that they had received T4A slips intended for someone else. On the same day, Advanced Education investigated the breach, identified the addressing error and mailed new T4A slips to the 277 students who it identified as having been affected.
- February 28, 2024 – A supervisor reported the breach to Advanced Education's privacy office. The privacy officer reported the matter to the Deputy Minister's office.
- April 24, 2024 – Advanced Education notified the affected parties. Details of the notice are discussed below.

- May 6, 2024 – Advanced Education's privacy officer reported the breach to my office.

- May 16, 2024 – On the advice of my office, Advanced Education wrote to the individuals who received the incorrect T4A slip asking them not to open the envelope and to email Advanced Education's privacy office to arrange for the return of the misdirected mail.

[25] Advanced Education further explained that to contain the breach it undertook the following:

- On the advice of my office, Advanced Education contacted Canada Post to gather information about how misaddressed envelopes were managed. Canada Post advised Advanced Education that where the postal code is the only error in the address, it manually corrects the postal code at the local delivery office.

- Also, on the advice of my office, Advanced Education wrote to the individuals who received the misdirected mail and asked them to email the privacy office to arrange for the return of the misdirected mail.

- Advanced Education advised that it received some responses from individuals advising that the mail was returned to Canada Post unopened, or having recognized the name of the person on the envelope it was delivered unopened by hand.

[26] As of the date of this Investigation Report, and assuming that Canada Post followed its normal practice of correcting postal codes, Advanced Education reported that there are 154 unaccounted for T4 slips that affected 121 individuals. It arrived at this number as follows:

Status	**No. of T4A slips**	**No. of Affected Individuals**
Misaddressed	415	277
Returned to Advanced Education	189	108
Wrong Postal Code Only	72	47
Unaccounted For	154	121

[27] As I said in paragraph [23] above, in assessing efforts to contain the breach, my office applies a reasonableness standard. Based on the information provided, I find that Advanced Education took reasonable steps to contain the breach. However, with 154 unaccounted for T4A slips, it appears that the breach was not completely contained.

Notify affected individuals (as soon as possible)

[28] Section 29.1 of FOIP requires government institutions to notify individuals when their personal information has been breached and a real risk of significant harm exists for the affected individuals.

[29] Section 29.1 of FOIP states:

> **29.1** A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[30] Even where section 29.1 of FOIP does not apply, unless there is compelling reason not to, a government institution should always notify affected individuals of a privacy breach. Trustees should follow the same practice.

[31] It is important to notify affected individuals for several reasons. Affected individuals have a right and need to know to protect themselves from any harm that may result. This is particularly important where sensitive information such as social insurance numbers are involved. As noted above, Advanced Education sent notice of the incident to the 277 individuals it originally thought were affected by the misdirected mail on April 24, 2024.

[32] My office's *Guide to FOIP*, Ch. 6 at pages 274 to 275, sets out the information that should be included in every notice to affected individual(s):

- 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 information.
- A notice that individuals have a right to complain to my office (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

[33] The notice sent by Advanced Education, a copy of which was provided to my office, described the information that was involved, described the cause of the breach in general terms and invited the affected parties to contact Advanced Education's privacy office and my office.

[34] The notice did not include a description of possible types of harm that may come to the affected individual, and advice on actions that they could take to further mitigate the risk of harm and protect themselves.

[35] The notification letters should have included a warning about the risk of identity theft and set out the actions that individuals could take to mitigate the risks. I recommend that, within 30 days of the issuance of this Investigation Report, Advanced Education amend its template for future breach notifications to include information about the risks that may arise from a breach and how to mitigate those risks.

[36] I note that the notification letters did not include offers to provide credit monitoring. In response to questions posed by my office, Advanced Education stated that the issue of offering credit monitoring in response to privacy breaches is "in review." However, in its Questionnaire, Advanced Education acknowledged that a social insurance number was sensitive and that it can be used to commit identity or financial fraud.

[37] Risks of identity theft are increasing as noted by the Canadian Anti-Fraud Centre (CAFC). In it 2022 Annual Report, the CAFC reported an increase in personal information theft and identity crimes. It stated, at page 44:

> The CAFC continues to see increases in personal information theft and identity crimes. In 2022, the CAFC received 8,086 reports of personal information theft and 19,543 reports of identity fraud, compared to 7,808 reports of personal information theft and 31,797 reports of identity fraud in 2021.
>
> Note: Identity fraud is used for financial gain. However, the CAFC is unable to accurately track how much money is lost to identity crimes through reports, as identifying information and individual identities can be used in many illicit ways that are not known by the victim at the time of reporting.

[38] In previous investigation reports of my office where social insurance numbers and banking information were involved, we have recommended credit monitoring. See for example: Investigation Report 153-2022, 164-2022, 168-2022, 169-2022, 170-2022, 195-2022, Investigation Report 200-2023 and Investigation Report 061-2023, 087-2023.

[39] In my office's Investigation Report 136-2024, 169-2024, 183-2024, 187-2024, 191-2024, I recommended that the credit monitoring be offered for 10 years after a cyber security breach involving over 7,000 affected parties. I stated:

> [38] … [G]iven my office's experience with investigating privacy breaches, I am now recommending that organizations offer affected individuals credit monitoring for a minimum of ten years, if not longer. Data is easily stored by threat actors and they may release individuals' information at any time, especially when individuals least expect them to do so.

[40] In my office's Investigation Report 208-2021, information including the driver's license number of one individual was mistakenly sent to another individual via email. The public body did not offer the affected individual credit monitoring and it was not included in my office's recommendations.

[41] In contrast, sensitive information, including social insurance numbers, was stored in boxes in paper format and left unsecured in a boardroom in my office's Investigation Report 153-2022, 164-2022, 168-2022, 169-2022, 170-2022, 195-2022. Even though the City of Saskatoon

could not determine if the records had been accessed, it offered one year of credit monitoring to 347 affected individuals. In that investigation report, I commended the City for offering the service.

[42] I recognize that the risks of identity fraud or theft are lower when comparing the circumstances of this case with those in a breach involving electronic databases and large numbers of affected parties. However, the circumstances here weigh in favour of a recommendation that credit monitoring be offered; namely, the sensitive nature of the information involved and the statistics regarding the increasing risks of identity theft by bad actors.

[43] Advanced Education's notice included some of the elements my office suggests. However, I find it should have included an offer of credit monitoring given the risk involved. I recommend that, within 30 days of the issuance of this Investigation Report, Advanced Education send a letter to the 121 affected parties whose T4A slips remain unaccounted for offering them credit monitoring for one year.

Investigate the breach

[44] After containing the breach and notifying affected parties, government institutions and trustees should conduct an internal investigation. My office's *Guide to FOIP*, Ch. 6 at page 275, describes an internal investigation as a methodical process of examination, inquiry, and observation including interviewing witnesses and reviewing documents. The purpose is to conduct a root cause analysis, which is a useful process for understanding and solving a problem, and to identify measures necessary to prevent further similar breaches.

[45] The *Guide to FOIP*, Ch. 6 at page 277, states that a root cause analysis seeks to identify the origin of a problem by using a specific set of steps and tools to:

- Determine what happened.
- Determine why it happened.

- Figure out what to do to reduce the likelihood that it will happen again.

[46] A root cause analysis should include a consideration of section 24.1 of FOIP. Section 24.1 of FOIP sets out the government institution's duty to protect personal information. This requirement includes establishing policies and procedures to maintain administrative, technical and physical safeguards. That provision states:

> **24.1** Subject to the regulations, a government institution 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.

[47] Similar requirements to protect personal health information appear in HIPA. Section 16 of HIPA states:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[48] As to the root cause of the breach, Advanced Education explained that the senior employee involved had been performing this task for twenty plus years. They had significant experience in the position but due to configuration changes in the Excel software that the employee was not aware of, the addressing errors were made. Advanced Education explained that the new version resulted in "the formula for incrementing numbers also modifying values in the address column." The last privacy training that the employee had participated in was in September of 2023.

[49] It stated that the lack of administrative safeguards to support or verify the accuracy of the address information and the fact that no training was provided on the new version of the Excel software used to prepare the address labels were the root causes of the breach. I agree with Advance Education's assessment of the root cause.

[50] It added that mailing T4A slips to physical addresses is not the preferred way to send sensitive personal information. However, it added that not all of its manual systems have been replaced. Advanced Education would prefer to deliver the tax slips online through a secure and tested system along with automating processes to reduce mistakes. I will speak to this further in the next section of this Investigation Report.

[51] I find that Advanced Education undertook an adequate investigation into the breach.

Take appropriate steps to prevent future breaches

[52] Once government institutions and trustees contain a breach and identify a root cause, they should consider and implement solutions that help prevent the same type of breach from occurring again. Prevention is one of the most important steps. A privacy breach cannot be undone but a government institution can learn from one and take steps to help ensure that it does not happen in the future.

[53] To prevent future breaches, Advanced Education stated that it is eliminating paper and mailing with the development of a system to automate delivery of tax slips. It is expected

to be in place in the fall of 2025. In the meantime, it has implemented a change in its paper process applicable to staff involved. This change requires that the last step in the paper mailing will be to check the address labels against the source system to ensure no unexpected changes have occurred when producing the labels. Advanced Education should ensure that the staff member who made the error which led to the breach and others who may be using the software or carrying out similar functions are apprised of any updated procedures and trained on the use of the new software.

[54] Advanced Education also stated that this privacy breach will be used in annual privacy training to help prevent future breaches of this kind.

[55] I find that the Advanced Education's plan to prevent future breaches of this nature is reasonable.

III FINDINGS

[56] I find that I have jurisdiction to investigate this matter under FOIP and HIPA.

[57] I find that a privacy breach occurred.

[58] I find that Advanced Education took reasonable steps to contain the breach.

[59] I find that Advanced Education's notices to the affected parties were not adequate.

[60] I find that the Advanced Education conducted an adequate investigation into the breach.

[61] I find that the Advanced Education's plan to prevent future breaches of this nature is reasonable.

IV RECOMMENDATIONS

[62] I recommend that, within 30 days of the issuance of this Investigation Report, Advanced Education amend its template for future breach notifications to include information about the risks that may arise from a breach and how to mitigate those risks.

[63] I recommend that, within 30 days of the issuance of this Investigation Report, Advanced Education send a letter to the 121 affected parties whose T4A slips remain unaccounted for offering them credit monitoring for one year.

Dated at Regina, in the Province of Saskatchewan, this 16th day of December, 2024.

Ronald J. Kruzeniski, K.C.
A/Saskatchewan Information and Privacy Commissioner