Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 061-2023, 087-2023

Ministry of Immigration and Career Training

September 6, 2023

Summary: The Ministry of Immigration and Career Training (Immigration) proactively reported two privacy breaches to the Commissioner's office. The reports stated that two Immigration employees had inappropriately accessed personal information contrary to *The Freedom of Information and Protection of Privacy Act*. The Commissioner investigated the incidents. He found that Immigration took appropriate and timely action to contain the breaches with one exception. He also found that Immigration's investigations were adequate, and with one exception, appropriately identified steps to be taken to prevent further breaches of this nature. However, he further found that Immigration's notices to the affected parties were not adequate. The Commissioner recommended that Immigration ensure that its notification letters inform affected parties about the risk of identity theft where the nature of the personal information involved, and other circumstances, raise such a risk. He recommended that, within 30 days of the issuance of this Investigation Report, Immigration offer five years of credit monitoring to those affected parties who may be at risk of identity theft. He also recommended that, within 30 days of issuance of this Investigation Report, Immigration amend its breach containment and investigation practices to include a requirement to ask if information had been printed or disclosed. In addition, he recommended that, within 30 days of issuance of this Investigation Report, Immigration commit to exploring the ability to audit employees' printing activities. Finally, the Commissioner recommended that, within 30 days of issuance of this Investigation Report, Immigration forward its investigation files to the Ministry of Justice and Attorney General, Public Prosecutions Division.

I BACKGROUND

[1] This Investigation Report considers two proactively reported privacy breaches involving two different employees of the Ministry of Immigration and Career Training

(Immigration). As the breaches involve similar circumstances, I have decided to issue one Investigation Report.

[2] The first breach (my office's Investigation File 061-2023) was reported to my office on March 6, 2023. Immigration reported that an employee (Employee 1) of its Immigration Services Branch had inappropriately accessed the personal information of 34 clients on Immigration's online immigration system. The records accessed related to the clients' immigration applications.

[3] The second breach (my office's Investigation File 087-2023) was reported to my office on March 29, 2023. Immigration reported that a different employee (Employee 2) of the same branch had inappropriately accessed the personal information of eight clients on Immigration's online immigration system.

[4] Immigration stated that the employees' actions were contrary to *The Freedom of Information and Protection of Privacy Act* (FOIP). In both cases, Immigration discovered the inappropriate accesses during an investigation that arose out of concerns about a potential conflict of interest on the part of the employees.

[5] Employee 1's inappropriate accesses occurred between January 2022 and December 2022. Employee 2's inappropriate accesses occurred between May 2021 and December 2021.

[6] On April 5, 2023, and April 17, 2023, my office notified Immigration that it would be conducting investigations into these matters. On May 19, 2023, and June 5, 2023, Immigration provided my office with its submissions.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[7] Immigration qualifies as a "government institution" pursuant to subsection 2(1)(d)(i) of FOIP.

[8] The privacy rules in FOIP only apply to personal information. Therefore, I must first determine if the information at issue qualifies as personal information under subsection 24(1) of FOIP (*Guide to FOIP*, Chapter 6: "Protection of Privacy", updated: February 27, 2023, [*Guide to FOIP*, Ch. 6], at page 31).

[9] Immigration stated that the information inappropriately accessed by Employees 1 and 2 included clients' names, contact details, information about their application for immigration, place and date of birth, education, work experience, family members, social insurance number, and financial information, such as information about bank accounts.

[10] In both cases, Immigration stated that the information was sensitive information. In relation to Employee 1's breach, Immigration's internal "Privacy Breach Incident Report Template" acknowledged that there was a risk of identity theft and stated that the information involved included "more than enough information to assume someone's identity." In relation to Employee 2's breach, Immigration did not indicate whether there was a risk of identity theft.

[11] Individuals' names and personal contact details would qualify as personal information pursuant to subsection 24(1)(e) of FOIP. Individuals' social insurance numbers would qualify as personal information pursuant to subsections 24(1)(d) and (k) of FOIP. Employment, financial and education related information would qualify as personal information under subsection 24(1)(b) of FOIP. Information about the individuals' family members, and place and date of birth would qualify as personal information pursuant to subsection 24(1)(a) of FOIP. These subsections 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*;
>
> (e) the home or business address, home or business telephone number or fingerprints of the individual;
>
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
>
> (ii) the disclosure of the name itself would reveal personal information about the individual.

[12] As Immigration is a government institution and personal information is involved in these breaches, I find that I have jurisdiction to investigate these matters under FOIP.

2. Did Immigration respond appropriately to this privacy breach?

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

[14] As set out in section 4-4 of my office's *Rules of Procedure* and my office's *Guide to FOIP*, Ch. 6, p. 267, my analysis of Immigration's responses to the privacy breaches involves a consideration of the following:

1. Containment of the breach
2. Notification of affected individuals
3. Investigation of the breach
4. Steps taken to prevent future breaches

[15] I turn to consider how Immigration followed each of these steps.

Containment of the breach

[16] Upon learning that a privacy breach has occurred, government institutions should immediately take steps to contain the breach. Depending on the nature of the breach, this can include:

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

(*Guide to FOIP*, Ch. 6, p. 268)

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

[18] Following is a timeline of key events in Immigration's investigation into the breach involving Employee 1:

- November 17, 2022 – Immigration identified a potential conflict of interest and began an investigation into Employee 1's activity reports for the period from January 2022 to December 2022.
- December 1 and 9, 2022 – Immigration met with Employee 1 and asked them to explain some accesses to "Program Integrity Files." These files were not assigned to Employee 1.
- December 2, 2022 – Immigration placed Employee 1 on administrative leave.
- December 29, 2022 – Immigration terminated Employee 1's employment.
- Early January 2023 – Immigration staff notified Immigration's Chief Privacy and Access Officer of the breach.

- February 2023 – Immigration's investigation found that Employee 1 had accessed files relating to 34 individuals. It also found that Employee 1 had no business-related purpose for accessing the files.

- March 6, 2023 – Immigration notified the affected individuals and my office.

[19] At the time of filing its submission, Immigration continued to investigate Employee 1's activity. Immigration subsequently advised my office that no additional instances of snooping by Employee 1 had been discovered and its investigation had concluded.

[20] Following is a timeline of the key events in Immigration's investigation into the breach involving Employee 2:

- March 2022 – Immigration became aware of Employee 2's work for an outside business.

- March 21, 2022, and January 14, 2023 – Employee 2 was on an approved leave of absence.

- January 16, 2023 – Employee 2 returned to work and was asked to submit a Conflict of Interest (COI) form given their work outside the Government of Saskatchewan.

- January 16, 2023 – Given Employee 2's work outside the Government of Saskatchewan and information on their resume, Immigration staff brought concerns about them to the attention of an Immigration Director.

- January 16, 2023 – Immigration discovered that Employee 2's outside employer was Employee 2's brother and the employer had active files with Immigration.

- January 16-17, 2023 – Immigration reviewed Employee 2's activities on Immigration's systems and discovered questionable activity that prompted a formal human resources investigation.

- January 20, 2023 – Employee 2 submitted their COI form to Immigration.

- January 27, 2023 – Immigration held a fact-finding meeting with Employee 2.

- January 30, 2023 – Immigration terminated Employee 2's access rights to Immigration's system.

- February 3, 2023 – Immigration held a second fact finding meeting to discuss additional suspicious activity. During this meeting, Employee 2 admitted to having

accessed files for three Immigration applicants and one employer without a business reason for doing so.

- March 7, 2023 – Immigration terminated Employee 2's employment.

[21] In relation to Employee 2, Immigration stated that it had no way to determine what if any information was copied from its system and what happened to that information.

[22] In the future, Immigration should ask employees suspected of snooping if any copies of records of personal information have been made and if any personal information in written or oral form has been shared. This was the approach taken by the Regina Public Library in my office's Investigation Report 108-2018, where it asked a third party for written assurances that they did not make or distribute copies of records of personal information that were involved in a breach. In some cases, it may be necessary to ask the snooping employee to provide an affidavit verifying their responses.

[23] Knowing if copies or information has been shared by a snooping employee is important as it will help public bodies determine if any further actions are required to contain the breach. Public bodies may not be able to determine with any certainty if the individual responds truthfully to their inquiries. However, by asking these questions, they will have made their best efforts to contain the breach.

[24] I find that Immigration took timely and adequate steps to contain the breach with the exception noted above. I recommend that, within 30 days of issuance of this Investigation Report, Immigration amend its breach containment and investigation practices to include a requirement to ask a snooping employee if they have printed or disclosed the information at issue.

Notification of affected individuals

[25] Section 29.1 of FOIP requires that, where there is an unauthorized use or disclosure of personal information, government institutions must notify the affected individual(s) if the "incident creates a real risk of significant harm" (*Guide to FOIP*, Ch. 6, p. 268).

[26] 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.

[27] Even where section 29.1 of FOIP does not apply, unless there is a compelling reason not to, government institutions should always notify affected individuals of a privacy breach.

[28] Immigration stated that it notified the 34 individuals affected by Employee 1's unauthorized accesses on March 7, 2023. It notified the eight individuals affected by Employee 2's unauthorized accesses on March 29, 2023.

[29] 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. Government institutions may also want to notify organizations, such as, my office, law enforcement or other regulatory bodies that oversee professions.

[30] A notice to affected individual(s) should include:

- 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 the IPC (provide contact information)
- Recognition of the impacts of the breach on affected individuals and, an apology

(*Guide to FOIP*, Ch 6, pp. 269)

[31] Employee 1's breach was confirmed during meetings with them on December 1 and 9, 2022. Employee 2's breach was confirmed on January 30 and February 3, 2023. In both cases, the letters notifying the affected parties were sent approximately three months after the breach was confirmed. I note that this was a significant improvement when compared to the time taken by Immigration to notify affected parties in my office's Investigation Report 032-2023.

[32] Immigration provided my office with a copy of its notification letters. Like the letters sent in Investigation Report 032-2023, the letters did not include a warning about the risk of identity theft. This warning should have been included in the letters sent to individuals affected by the breaches. Immigration's own internal "Privacy Breach Incident Report Template" relating to Employee 1 stated that the personal information involved included "more than enough information to assume someone's identity."

[33] The internal "Privacy Breach Incident Report Template" relating to Employee 2 identified the information involved as sensitive. It did not say anything about the risk of identity theft. Given that the personal information involved appeared to be similar to the information involved in Employee 1's breach, the risk of identity theft would also exist for these affected individuals.

[34] In these circumstances, the notices to affected parties in both breaches should have informed them that there was a risk of identity theft and set out the actions they could take to address it.

[35] I recommended that Immigration address the issue of identity theft in its notification letters in Investigation Report 032-2023. In response, Immigration did not agree to "address the issue of identity theft" in its letters. It stated:

> ICT will continue to include the personal information that is the subject of the suspected privacy breach in its notification letters. ICT will also continue to provide contact information of an ICT employee, so that the affected individuals know who to contact if they have more questions or have concerns they want addressed.

[36] In the previous reports where identity theft has been a risk, such as my office's Investigation Report 370-2021, I have also found government institutions should offer affected parties credit monitoring for a minimum of five years. In response to a similar recommendation made in Investigation Report 032-2023, Immigration stated that it would consider the recommendation.

[37] For the reasons set out above, I find that Immigration's notice to the individuals affected by the breaches in this case was not adequate.

[38] As Immigration decided not to comply with the related recommendations made in Investigation Report 032-2023, I will repeat them here. I recommend that, in the future, Immigration ensure that its notification letters inform affected parties of the risk of identity theft where the nature of the personal information involved, and other circumstances raise that risk. I also recommend that, within 30 days, Immigration offer five years of credit monitoring to those affected parties who may be at risk of identity theft.

Investigation of the breach

[39] After containing the breach and notifying affected parties, government institutions should conduct an internal investigation. An internal investigation is 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. It seeks to identify the origin of a problem by using a specific set of steps and tools to:

- determine what happened,
- determined why it happened, and
- figure out what to do to reduce the likelihood that it will happen again.

(*Guide to FOIP*, Ch. 6, pp. 269-274)

[40] As to the root cause of the breach involving Employee 1, Immigration appears to point to the lack of role-based access controls. It stated that the positions held by this employee did not require them to access program integrity records. It added that this did not appear to be a case of accidental access.

[41] Immigration appears to suggest that that the root cause of Employee 2's breach was similar. It asserted:

> Each staff member is assigned roles in the online application system that allows them access to specific client information that they need for their job. In some instances, a role(s) may allow them to access information that they do not need due to the current structure of the online application. Staff are instructed during orientation and training and through the Freedom of Information and Protection of Privacy training taken by all Government of Saskatchewan employees that they must only access client information as needed to do their duties.

[42] I agree that the lack of role-based access controls contributed to the breach. However, in both cases, the breaches were discovered after Immigration became aware of conflicts of interest. While Immigration's submission does not specifically identify conflict as one of the root causes, it appears that it did consider this given the actions taken by it to provide further guidance and training on its conflict-of-interest policies. I will address this in the section that follows.

[43] I find that Immigration's investigation into the breach was adequate.

Take appropriate steps to prevent future breaches

[44] Once government institutions 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. To avoid future breaches, government institutions should make a prevention plan.

[45] To prevent future breaches, Immigration's internal "Privacy Breach Incident Report Template" relating to Employee 1's breach stated:

> A Risk Management Action Plan has been developed and is going through internal review/feedback. The action plan includes preventative measures to be taken to safeguard the program further, including system changes to further lock down staff roles.

[46] In its submission relating to Employee 1, Immigration expanded on its plan to prevent further breaches of this nature. It stated:

> As a result of this and other recent breaches, steps have been taken to improve processes and reporting requirements and upgrades are currently underway or in development to implement system changes to address concerns that have been raised. The system will have barriers installed to reduce the risk of employees accessing information they do not need for their job duties.
>
> The online system vendor was able to create a report that can be run by senior management staff to track, review and audit staff activity in the system, instead of needing to request special reports from the vendor. This activity report was used to review [Employee 1's] activity in the online system. These reports now allow the management staff to proactively audit staff on a regular basis and enhance the ministry's ability to identify breaches in a more effective manner. The new, updated report includes the ability to track when staff make changes in [the system], as well as when they view a record.

[47] It added that a conflict of interest and privacy training session was held for all staff on January 25, 2023. "Conflict of Interest Guidelines" were developed for all staff and distributed in April 2023. Privacy training that focuses on snooping is being developed and will be delivered in early fall 2023. A recommendation will be made to the Deputy Minister to make the training mandatory on an annual basis. In addition, Conflict of Interest and Privacy training will be offered to all new Immigration Services Branch staff on a quarterly basis. Finally, Immigration will work with the Attorney General to determine if prosecution under FOIP in relation to Employee 1 is warranted.

[48] In relation to Employee 2's breach, Immigration's internal "Privacy Breach Incident Report Template" referred to the Risk Management Action Plan described above and the work to limit staff access to information in its system based on their roles. It also stated that Management staff have begun auditing staff and are working on a formal audit plan.

[49] I find that the proposed steps to be taken by Immigration to prevent future breaches are appropriate with one exception. In light of my findings above about the need for further information regarding if snooping employees printed or shared records or information, I recommend that, within 30 days of issuance of this Investigation Report, Immigration commit to exploring the feasibility of auditing employees' printing activities in relation to its online immigration system.

[50] As noted above, Immigration stated that it will be referring the breach related to Employee 1 to the Ministry of Justice and Attorney General, Public Prosecutions Division (PPD) to determine if a prosecution is warranted. It did not indicate if it would be doing so in relation to Employee 2. If it has not already done so, I recommend that Immigration forward both investigation files, including the internal investigations, to the PPD. This will allow prosecutors to consider if any offences under FOIP have occurred and if charges should be laid under that act or any other statute against Employee 1 and/or 2.

III FINDINGS

[51] I find that I have jurisdiction to investigate these matters under FOIP.

[52] I find that Immigration took appropriate and timely action to contain the breaches except for its failure to make inquiries about printing and sharing of personal information.

[53] I find that Immigration's notices to the affected parties were not adequate.

[54] I find that Immigration's investigations were adequate.

[55] I find that Immigration has appropriately identified steps to be taken to prevent further breaches of this nature.

IV RECOMMENDATIONS

[56] I recommend that in the future, Immigration ensure that its notification letters inform affected parties about the risk of identity theft where the nature of the personal information involved, and other circumstances, raise such a risk.

[57] I recommend that, within 30 days of issuance of this Investigation Report, Immigration offer five years of credit monitoring to those affected parties who may be at risk of identity theft.

[58] I recommend that, within 30 days of issuance of this Investigation Report, Immigration amend its breach containment and investigation practices to include a requirement to ask a snooping employee if they have printed or disclosed the information at issue.

[59] I recommend that, within 30 days of issuance of this Investigation Report, Immigration commit to exploring the ability to audit employees' printing activities in relation to its online immigration system.

[60] I recommend that, within 30 days of issuance of this Investigation Report, Immigration forward its investigation files, to the Ministry of Justice and Attorney General, Public Prosecutions Division, if it has not already done so.

Dated at Regina, in the Province of Saskatchewan, this 6th day of September, 2023.

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