Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 216-2018, 218-2018

Ministry of Immigration and Career Training

June 19, 2019

Summary: The Ministry of Immigration and Career Training (Immigration and Career Training) proactively reported a privacy breach to the Office of the Information and Privacy Commissioner (IPC). Shortly thereafter, the IPC received a complaint from one of the affected individuals of the privacy breach. According to Immigration and Career Training, an auditor with the Office of the Provincial Auditor of Saskatchewan was involved with a routine audit at Immigration and Career Training. Upon completion of the audit, Immigration and Career Training discovered the auditor had accessed information on three applications in the Saskatchewan Immigrant Nominee Program that were not on the list provided by the auditor. The Commissioner found that Immigration and Career Training appropriately handled the privacy breach in accordance with the five best practice steps. The Commissioner recommended that Immigration and Career Training take no further action.

I BACKGROUND

[1] On October 2, 2018, the Ministry of Immigration and Career Training (Immigration and Career Training) contacted my office to proactively report a breach of privacy. Immigration and Career Training advised that an auditor with the Office of the Provincial Auditor of Saskatchewan was involved in a routine audit at Immigration and Career Training. The auditor was granted electronic access to the Saskatchewan Immigrant Nominee Program (SINP) database called OASIS in order to conduct an audit. The auditor provided Immigration and Career Training with a list of the individuals whose files would be audited. Immigration and Career Training discovered that the auditor accessed information on three SINP applications that were not on the list. Immigration and Career

Training was able to determine that the auditor accessed the auditor's own personal information five times, as well as two other individuals.

[2] By way of letter dated October 1, 2018, Immigration and Career Training notified the two affected individuals.

[3] On October 5, 2018, my office received a complaint from one of the affected individuals (the Complainant). When a complaint is received from an affected individual following a proactively reported breach, in the interest of transparency, my office automatically issues an investigation report on the matter.

[4] On October 12, 2018, my office notified Immigration and Career Training and the Complainant that it would be investigating the matter and requested a copy of Immigration and Career Training's internal investigation report. On October 25, 2018, my office received an internal investigation report from Immigration and Career Training.

[5] On January 23, 2019, my office also received an internal investigation report from the Office of the Provincial Auditor of Saskatchewan. The report outlined steps the Office of the Provincial Auditor of Saskatchewan took in response to the privacy breach incident. My office did not request a report, it was provided as a courtesy. My office appreciates that the Provincial Auditor provided additional information.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] Immigration and Career Training is a "government institution" pursuant to subsection 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP). Thus, I have jurisdiction to conduct this investigation. I also have jurisdiction to investigate how Immigration and Career Training handled this breach of privacy.

2. Is there personal information involved?

[7] In order for the privacy provisions under FOIP to be engaged, the data elements at issue must constitute personal information. According to the internal investigation report received from Immigration and Career Training, the data elements involved are:

- SINP Applicant name;
- Application number;
- Current Country of Residence;
- Residency Status at application; and
- Settlement destination in Saskatchewan.

[8] According to Immigration and Career Training, no other information was accessible to the auditor.

[9] Subsection 24(1) of FOIP defines what qualifies as personal information. Specifically, subsections 24(1)(d) and (k)(i) of FOIP provide that any identifying number assigned to an individual or the name where it appears with other personal information qualifies as personal information pursuant to these provisions. Subsections 24(1)(d) and (k)(i) of FOIP provide:

> **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:
> …
> (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;
> …

[10] The data elements involved constitute personal information of the affected individuals pursuant to subsections 24(1)(d) and (k)(i) of FOIP. Therefore, there is personal information involved in this matter.

3. Did Immigration and Career Training respond appropriately to the privacy breach?

[11] In circumstances where a government institution proactively reports a privacy breach, the focus for my office becomes one of determining whether the government institution appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that Immigration and Career Training took the privacy breach seriously and appropriately addressed it. My office recommends five best practice steps be taken when a government institution discovers a breach of privacy has occurred. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Plan for prevention; and
5. Write an investigation report.

[12] I will now consider the appropriateness of Immigration and Career Training's handling of the matter against these five best practice steps.

Step 1: Contain the breach

[13] Upon learning that a privacy breach has occurred, a government institution 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 access privileges; or
- Correcting weaknesses in physical security.

[14] Effective and prompt containment reduces the magnitude of a breach and in some instances, the risks to an individual.

[15] In its internal investigation report, Immigration and Career Training advised that as per normal practice, the auditor's access to the system was revoked when the necessary tasks in OASIS were completed.

Step 2: Notify affected individuals and/or appropriate organizations

[16] Notifying an individual that their personal information was inappropriately accessed is important for a number of reasons. Not only do individuals have a right to know, they need to know in order to protect themselves from any potential harm that may result from the inappropriate access. Unless there is a compelling reason not to, government institutions should always notify affected individuals. An effective notification should include:

- A description of what happened;
- A detailed description of the personal information that was involved;
- A description of possible types of harm that may come to them as a result of the privacy breach;
- Steps that the individuals can take to mitigate harm;
- Steps the organization is taking to prevent similar privacy breaches in the future;
- The 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 the Office of the Information and Privacy Commissioner; and
- Recognition of the impacts of the breach on affected individuals and an apology.

[17] In addition to notifying individuals, government institutions may want to notify other organizations, for example, my office, law enforcement or other regulatory bodies that oversee particular professions.

[18] Immigration and Career Training provided notification to the two affected individuals by way of letter dated October 1, 2018. I reviewed the letter and it contained most of the elements recommended by my office.

[19] Immigration and Career Training also notified my office of the breach. It also immediately notified the Office of the Provincial Auditor of Saskatchewan who took steps internally with its employee.

Step 3: Investigate the breach

[20] Once the breach has been contained and appropriate notification has occurred, the government institution should conduct an internal investigation. The government institution's Privacy Officer generally conducts the investigation because they have the appropriate privacy expertise to do so and understand what the relevant privacy legislation requires of their organization. The investigation should address the incident on a systemic basis and should include a root cause analysis. The investigation should be documented in an internal privacy breach investigation report. At the conclusion of its investigation, the government institution should have a solid grasp on what occurred.

[21] Immigration and Career Training provided an internal investigation report. It was detailed and included the necessary information. According to the report, on September 12th and 13th, 2018, an auditor with the Office of the Provincial Auditor of Saskatchewan was granted electronic access to OASIS. The auditor was conducting an audit of the Entrepreneur Program. The auditor provided Immigration and Career Training with a list of the individuals whose files would be audited. The auditor had full access to the Entrepreneur Program files, but limited access to any other program within OASIS. The OASIS database is designed with electronic safeguards that restrict the information that is accessible based on roles. Once the auditor completed the necessary tasks in OASIS, access was revoked. As the auditor was not an employee of Immigration and Career Training, steps were taken to conduct an activity audit. The activity audit was received and reviewed on September 17, 2018 and it revealed that on September 12, 2018, the auditor accessed the auditor's own personal information five times. It also revealed that the applications of two other individuals were accessed. None of the information was part of the list of the individuals whose files were to be audited.

[22] As noted earlier in this report, Immigration and Career Training alerted the Office of the Provincial Auditor of Saskatchewan who then interviewed the auditor. The auditor admitted to looking at the applications and displayed remorse. Through both the investigation by Immigration and Career Training and the Office of the Provincial Auditor of Saskatchewan, it was learned that the auditor knows the Complainant and the other affected individual so the information viewed was not random. It appeared the reason for viewing the information was curiosity. There did not appear to be any malicious intent. No additional information was accessed.

[23] The Office of the Provincial Auditor of Saskatchewan determined that the incident was a serious breach of employment duties and the policies of its office. A number of terms were set which the auditor agreed to. This included a period of suspension, followed by a period of probation, review of all policies and standards of conduct within a specified time and a warning that any further incidents of a similar nature would result in immediate dismissal.

Step 4: Plan for prevention

[24] Prevention is perhaps one of the most important steps. A privacy breach cannot be undone but a government institution can learn from one and improve its practices. To avoid future breaches, a government institution should formulate a prevention plan. Some changes that are needed may have revealed themselves during the investigation phase. For example, deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training.

[25] Immigration and Career Training indicated that there are currently internal processes and procedures that assist in identifying breaches of privacy quickly. The OASIS database has the capability to document who has accessed records. This system is set up to identify when snooping occurs and can accurately determine which files were breached and when. In addition, Immigration and Career Training has internal privacy breach protocols to ensure affected individuals are notified quickly.

[26] Despite these existing safeguards, Immigration and Career Training will also now implement a declaration form which will be used with non-ministry employees. All non-ministry employees will be required to sign the declaration prior to access to any systems being granted. A copy of the declaration form specific to audits was provided to my office for review. The declaration is clear and thorough. It includes notice that access will be monitored for consistency.

[27] The Office of the Provincial Auditor of Saskatchewan provided my office with a courtesy report on the steps it took. It reported that it has well-defined policies and processes around confidentiality of information. Further, it expects all employees to meet the requirements of its Code of Conduct, policies and professional standards when conducting work outside of its office. Staff are required annually to sign that they have read and understood the policies and must follow them. It reviewed its orientation training for new staff to ensure there was sufficient focus on privacy and confidentiality policies of the office. Some adjustments were made to simplify language. A Confidentiality Information Session was delivered to all staff during the office's annual training program in October 2018.

[28] In conclusion, I find that Immigration and Career Training responded appropriately to the privacy breach. My office is satisfied that the five best practice steps were followed. It appears that both Immigration and Career Training and the Office of the Provincial Auditor of Saskatchewan took the privacy breach seriously.

III FINDING

[29] I am satisfied with how Immigration and Career Training addressed this privacy breach.

IV RECOMMENDATION

[30] I recommend that Immigration and Career Training take no further action.

Dated at Regina, in the Province of Saskatchewan, this 19th day of June 2019.

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