Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 127-2022

Ministry of Immigration and Career Training

January 6, 2023

Summary: The Ministry of Immigration and Career Training (Ministry) sent an email to approximately 200 individuals without using the blind carbon copy field for the email addresses. One of the affected individuals filed a complaint with the Commissioner. The Commissioner found that personal information is involved and that a privacy breach occurred. The Commissioner found the Ministry did not take adequate steps to contain the privacy breach. The Commissioner recommended that the Ministry request the email recipients delete the email, request confirmation that it has been deleted and request the email is not forwarded to others. The Commissioner also found the Ministry properly notified the affected individuals of this privacy breach. The Commissioner found the Ministry conducted an adequate investigation into this privacy breach. Finally, the Commissioner found the Ministry took adequate steps to prevent future breaches.

I BACKGROUND

[1] On June 14, 2022, the Complainant submitted a privacy complaint to the Ministry of Immigration and Career Training (Ministry) as follows:

> I am forwarding this email to you as proof that my email address (which includes my first and last name) has been disclosed to about 200 people because Bcc wasn't used when the email was sent. You have 30 days to conduct an internal investigation and to provide a response.

[2] On June 17, 2022, the Ministry responded to the complaint. The response explained what happened and provided the Complainant with the contact information for the Ministry's Privacy Officer. In addition, it provided contact information for my office.

[3] As the Complainant was not satisfied with the response they received, they requested my office undertake an investigation on June 21, 2022.

[4] By emails on July 7, 2022, my office notified the Ministry and the Complainant that my office would be undertaking an investigation into this matter.

[5] On September 9, 2022, the Ministry provided my office with its response to the investigation.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] The Ministry is a "government institution" pursuant to subsection 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP). Therefore, I find I have jurisdiction to conduct this investigation.

2. Is personal information involved and did a privacy breach occur?

[7] In their June 21, 2022 complaint to my office, the Complainant asserts:

> On June 14, 2022, [Employee] sent out an email to about 190 people, including me, without using BCC and therefore this email included my first and last name and email address and implies that I received service for career development.

[8] From a review of the email, I can confirm the Ministry sent it to approximately 200 separate email addresses, including the Complainant's, in the "To" field. I can also confirm the Complainant uses their first and last name in their email address. The email was sent by a Career Services Consultant (Consultant) advising the individuals of a leave of absence they were taking and that another consultant would be taking over their caseload.

[9] These are important details as FOIP is engaged when there is personal information as defined in subsection 24(1) of FOIP. Subsection 24(1) provides an enumerated list of types

on information that would qualify as personal information. However, the list is non-exhaustive. In order to qualify as personal information, there must be 1) an identifiable individual, and 2) the information must be personal in nature. Specifically, subsection 24(1)(b) of FOIP provides:

> **24**(1) Subject to subsections (1.1) and (2), **"personal information"** mean 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;

[10] First, there is an identifiable individual as the Complainant's first and last name makes up part of their email address. Second, the email was sent to approximately 200 individuals from the Consultant. From the content of the email, the inference can be made that those receiving the email are part of the Consultant's caseload and, as such, has received some training or career development support from the Consultant. This information is personal in nature and qualifies as personal information pursuant to subsection 24(1)(b) of FOIP as it constitutes the education and/or employment history of the Complainant.

[11] Therefore, I find that personal information is involved and that FOIP is engaged. As the disclosure of the personal information was not authorized, I also find that a privacy breach occurred, which the Ministry does not deny. In the next section of this Investigation Report, I will consider the actions taken by the Ministry to respond to the privacy breach.

3. Did the Ministry respond appropriately to this privacy breach?

[12] As set out in my office's *Rules of Procedures*, when my office determines there has been a privacy breach, my office will analyze whether the government institution appropriately managed the breach by considering if it:

- Contained the breach (as soon as possible);
- Notified affected individuals (as soon as possible);

- Investigated the breach; and
- Taken appropriate steps to prevent future breaches.

[13] I will use these four steps to assess the Ministry's response to the breach.

Contained the breach (as soon as possible)

[14] Soon after a government institution learns of a privacy breach, it should contain and recover any personal information that is involved. This will require determining how broad the privacy breach is and what type of records are involved.

[15] The Ministry advised my office that it took the following steps to attempt to contain the privacy breach:

> The ICT employee attempted to do a recall of the email, however this was unsuccessful as the email addresses were outside of the Government of Saskatchewan. The recall was unsuccessful for some of the email addresses due to the fact that some were undeliverable.

[16] The breach was a result of a mass email being sent to approximately 200 employees and attempts to recall were not successful for all the email addresses it was sent to. Therefore, the Ministry concluded they were not able to fully contain the breach.

[17] The Ministry did notify all of the email recipients of the breach, which I will discuss in the next part of this report. However, the notification did not ask the email recipients to delete the email that was sent or ask for confirmation that it was deleted. It also did not request that the recipients not disseminate the email to others.

[18] As these additional steps were not taken, I find the Ministry did not take adequate steps to contain the privacy breach. I recommend the Ministry request the email recipients delete the email, request confirmation that it has been deleted and request the email is not forwarded to others.

Notified affected individuals (as soon as possible)

[19] Notice to affected individuals should happen as soon as possible when learning of a breach. Notifying an individual that their personal information has been inappropriately accessed or disclosed 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 potential harm that may result from the inappropriate disclosure. Unless there is compelling reason not to, government institutions should always provide notification.

[20] My office's *Privacy Breach Guidelines for Government Institutions and Local Authorities* (*Privacy Breach Guidelines*) suggests the following elements be included in notification to affected individuals on page 6:

- 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 them as a result of the privacy breach;
- steps taken and planned to mitigate the harm and to 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, how to change a health services number or driver's license number etc.);
- contact information of an individual within your organization who can answer questions and provide further information;
- a notice that individuals have a right to complain to the IPC (provide contact information); and
- recognition of the impacts of the breach on affected individuals and, an apology.

[21] In this matter, the Ministry advised my office it notified the affected individuals by sending two emails. One was sent to those whose names could be identified from their email addresses and the second, whose name was not part of their email address.

[22] The notification emails were sent to the affected individuals on June 17, 2022 and June 21, 2022 and included the following:

- An explanation of what happened;
- An explanation of what steps are being taken to mitigate the risk of this happening again;
- The contact information for the Ministry's Privacy Officer;
- The contact information for my office; and
- An apology.

[23] In addition, the Manager of the Consultant spoke with the Complainant on June 21, 2022:

> …An apology was made to the [Complainant] for the privacy breach. [They] was told that we take privacy breaches very seriously and have worked with the Consultant to educate and ensure that this type of breach does not happen in the future. [Complainant] was informed that notification of the breach was sent to each person affected….

[24] The Ministry has taken the necessary steps to properly notify the affected individuals of this matter. As such, I find the Ministry properly notified the affected individuals of this privacy breach.

Investigate the breach

[25] Investigating the privacy breach to identify the root cause is key to understanding what happened. Identifying the root cause will help prevent similar breaches in the future. The internal investigation should also consider whether the safeguards that were in place at the time of the incident were adequate.

[26] The Ministry advised my office that it took the following steps to investigate this matter:

> On June 15, 2022, the Manager of the unit reached out to question the employee about this situation. The employee is going on a leave of absence and used a mass email to communicate the leave to clients assigned to the employee. The employee did not use the blind carbon copy feature. The employee added all email addresses to the To: field.

> This allowed all email recipients to see each other's email addresses. Most email addresses also contained the first and/or las name of the client or another individual. The employee was not aware of how to use the blind carbon copy function.

[27] The Ministry advised that the Consultant has taken the following privacy training:

- September 14, 2021: Access and Privacy in the Government of Saskatchewan.
- December 16, 2021: Freedom of Information and Protection of Privacy for the Ministries of Trade and Export Development, Energy and Resources and Immigration and Career Training.
- Initial onboarding training that includes a section of privacy and snooping (FOIP and *The Health Information Protection Act*).

[28] From a review of the Ministry's investigation, it appears the root cause of this incident was caused from the Consultant not being aware of the blind carbon copy feature when sending an email.

[29] Section 24.1 of FOIP requires a government institution to establish administrative, technical and physical safeguards to protect personal information. As outlined in my office's *Privacy Breach Guidelines*, *administrative safeguards* are controls that focus on internal organization polices, procedures, and maintenance of security measures that protect personal information. By not using the blind carbon copy field when they sent the mass email, the Consultant was not following administrative safeguards to protect personal information.

[30] As a result of this breach of privacy, the Ministry has taken steps to mitigate the risk of a breach of this nature occurring in the future. I will discuss these steps in the next section of this report.

[31] I find the Ministry conducted an adequate investigation into this privacy breach.

Prevent future breaches

[32] In responding to a breach of privacy, it is important that a government institution take steps to mitigate the risk of a similar breach occurring in the future. The following are some steps that can be taken:

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

[33] The following are some of the steps taken by the Ministry to mitigate the risk of this type of breach occurring in the future:

- Regular reminders about privacy will be provided to staff.
- The branch concluded that sending mass emails to clients is a practice that will be discontinued.
- The employee was taught how to use the blind carbon copy filed in emails when sending out emails to multiple recipients in the event it would be required.
- The Consultant was required to retake privacy training.

[34] These are appropriate steps to take to prevent a future breach such as this from re-occurring.

[35] I would also note that from a review of the investigation materials provided to my office, the Ministry responded to this privacy breach quickly and took the matter very seriously. I would like to commend the Ministry for this.

[36] I find the Ministry took adequate steps to prevent future breaches.

III FINDINGS

[37] I find I have jurisdiction to conduct this investigation.

[38] I find that personal information is involved and that a privacy breach occurred.

[39] I find the Ministry did not take adequate steps to contain the privacy breach.

[40] I find the Ministry properly notified the affected individuals of this privacy breach.

[41] I find the Ministry conducted an adequate investigation into this privacy breach.

[42] I find the Ministry took adequate steps to prevent future breaches.

IV RECOMMENDATION

[43] I recommend that the Ministry request the email recipients delete the email, request confirmation that it has been deleted and request the email is not forwarded to others.

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

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