Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 083-2023

Saskatchewan Government Insurance

October 26, 2023

Summary: Saskatchewan Government Insurance (SGI) notified the affected individual (Complainant) that a privacy breach had occurred when an employee shared their personal information with another customer by mistake. The Complainant was not satisfied with SGI's notification and asked the Commissioner to investigate. The Commissioner found that a privacy breach occurred as the disclosure was unauthorized. The Commissioner also found that SGI managed the privacy breach appropriately for the most part. The Commissioner recommended that SGI explore ways to ensure employees follow policies and procedures.

I BACKGROUND

[1] On February 9, 2023, an employee of Saskatchewan Government Insurance (SGI) sent an email (with attachment) containing personal information of customer A to customer B by mistake.

[2] On February 22, 2023, customer B, who received the email with the attachment, contacted SGI and reported this incident.

[3] On February 28, 2023, SGI notified the affected customer A that their personal information was inadvertently shared with customer B.

[4] On March 22, 2023, the affected customer A (Complainant) requested that my office investigate this matter.

[5] On April 17, 2023, my office notified SGI and the Complainant of my office's intention to undertake an investigation. My office requested a copy of SGI's internal investigation report regarding this matter. My office also invited the Complainant to provide any further details regarding the alleged breach of privacy.

[6] On May 16, 2023, SGI provided its completed "Privacy Breach Investigation Questionnaire for Public Bodies" (Privacy Breach Questionnaire) to my office. The Complainant did not provide any further information to my office.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[7] SGI qualifies as a "government institution" pursuant to section 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP) and subsection 3(a) and Part I of the Appendix of *The Freedom of Information and Protection of Privacy Regulations*. Therefore, I have jurisdiction to conduct this investigation.

2. Did a privacy breach occur?

[8] For FOIP to be engaged in a privacy breach, there must be personal information involved as defined by section 24(1) of FOIP.

[9] SGI provided my office with a copy of the letter and attachment that it had provided to customer B by mistake. The letter contained the Complainant's claim number and the date of collision. The attachment contained injury forms with the Complainant's customer number (driver's license number), name, address and date of birth completed. The remaining fields on the injury form were blank (i.e., not completed).

[10] SGI did not cite any part of subsection 24(1) of FOIP in this matter; however, the data elements noted above would qualify as "personal information" as defined by subsections 24(1)(a), (d), (e) and (k)(i) of FOIP, which provide as follows:

> **24**(1) Subject to sections (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, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> …
> (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

[11] Therefore, I find that the Complainant's personal information is involved pursuant to subsections 24(1)(a), (d), (e) and (k)(i) of FOIP. As FOIP is engaged, the privacy rules outlined in Part IV of FOIP will guide this investigation.

[12] Section 29(1) of FOIP provides as follows:

> **29**(1) No government institution shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except in accordance with this section or section 30.

[13] Section 29 of FOIP prohibits the disclosure of personal information unless the individual about whom the information pertains consents to its disclosure or if disclosure without consent is authorized by one of the enumerated subsections of 29(2) or section 30 of FOIP (*Guide to FOIP*, Chapter 6, "Protection of Privacy", updated January 18, 2023 [*Guide to FOIP*, Ch. 6], p. 183).

[14] "Disclosure" is sharing of personal information with a separate entity, not a division or branch of the government institution in possession or control of that information (*Guide to FOIP*, Ch. 6, p. 183).

[15] "Consent" means voluntary agreement by a person in the possession and exercise of sufficient mental capacity to make an intelligent choice to do something proposed by another; it supposes a physical power to act, a moral power of acting and a serious, determined, and free use of these powers (*Guide to FOIP*, Ch. 6, p. 184).

[16] In this case, SGI agreed that it disclosed the Complainant's personal information by mistake to another customer. As the disclosure was unauthorized, I find that a privacy breach occurred.

3. Did SGI respond appropriately to the privacy breach?

[17] At this stage, my office moves on to considering how the government institution managed the privacy breach. My office will analyze whether the government institution properly managed the breach and took the following steps in responding to it:

- Contained the breach (as soon as possible).
- Notified affected individuals (as soon as possible).
- Investigated the breach.
- Prevented future breaches.

(*Guide to FOIP*, Ch. 6, p. 267)

[18] Based on the information that SGI provided to my office, I will now assess how it addressed each of these four steps. I will make any recommendations, as necessary, following my analysis of each of the four steps.

Contained the breach (as soon as possible)

[19] It is important to contain the breach immediately. In other words, ensure that personal information is no longer at risk. This may involve:

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

(*Guide to FOIP*, Ch. 6, p. 267)

[20] SGI explained that the privacy breach occurred on February 9, 2023, when it sent an email containing personal information of the Complainant to customer B by mistake. SGI did not realize that a privacy breach had occurred until February 22, 2023, when customer B contacted its staff and reported the error.

[21] SGI explained that it inquired with customer B, who confirmed that they had deleted the email (inbox and trash), they received in error.

[22] I find that SGI took appropriate steps to contain the privacy breach.

Notified affected individuals (as soon as possible)

[23] Notification to individuals affected by the breach should occur as soon as possible after key facts about the breach have been established. It is best to contact affected individuals directly, such as by telephone, letter, or in person. However, there may be circumstances where it is not possible, and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include: a notice

on a website, posted notices, media advisories and advertisements. Ensure the breach is not compounded when using indirect notification (*Guide to FOIP*, Ch. 6, p. 268).

[24] Notifications should include the following:

- 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).
- 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).
- Recognition of the impacts of the breach on affected individuals and, an apology.

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

[25] SGI explained that as the disclosure was made by mistake, the incorrect recipient contacted SGI to advise of the mistake, and confirmed they deleted the email (inbox and trash). SGI then concluded that there was no risk of significant harm to the Complainant due to this privacy breach. However, SGI did notify the Complainant on February 28, 2023.

[26] My office noted that SGI's notification letter to the Complainant listed the following:

- Explained how the privacy breach had occurred.
- What data elements of the complaint's personal information were affected.
- Provided a copy of the document shared in error.

- Informed the complainant that the customer who had received this information in error confirmed that they had deleted the email (inbox and trash).
- Explained how SGI concluded that it did not expect any harm to the complainant.
- Apologized to the complainant for this privacy breach.
- Provided contact information of SGI's manager of injury claims division.
- Provided the complainant with contact information for my office.

[27] I am satisfied that SGI's letter contained the elements that my office recommends. Based on the above, I find that SGI provided an adequate notification to the Complainant.

Investigated the breach

[28] Once a breach has been contained the next step is to investigate the breach. Here are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach.
- What occurred.
- How did the privacy breach occur.
- What is the applicable legislation and what specific sections are engaged.
- What safeguards, policies, and procedures were in place at the time of the privacy breach.
- Was the duty to protect met.
- Who are the affected individuals.

(*Guide to FOIP*, Ch. 6, pp. 269 - 271)

[29] As stated previously in this Investigation Report, SGI stated it was not aware it had breached the Complainant's privacy until customer B reported the incident to SGI. At that point, it investigated, stating as follows:

> On Feb.22/23 the manager of Saskatoon Injury Claims, [name of Manager] (LF) advised [name of the Privacy & Information Manager] (RT) of Privacy & Information Management (PIM) by email that a breach had occurred. RT immediately opened an investigation and sent an email asking the manager LF how this happened, and she advised that she was unsure – either there were two files open, or the documents in question, which were blank, were generated on the wrong file in GIS (General Insurance System), attached to the wrong file and were then attached to the email to the third party. LF further advised that same date that the third party had confirmed deletion of the email. On Feb. 23/23, RT advised LF that because the customer number was shown on one document, that notification to the affected individual would be appropriate. On Feb. 27/23 breach notification wording was drafted by RT and provided to LF, with the direction to send the letter to the affected individual; LF sent the letter to the complainant the same date and provided a copy to RT. Further discussions determined that it was more likely that the documents were accidentally generated on the complainant's file, attached to the third party's file, then attached to the email to the third party. The documents, which would have been attached to the third party file when the email was sent, were deleted off the third party file on Feb. 23/23.

[30] Pursuant to section 24.1 of FOIP a government institution has a duty to protect personal information in its possession or under its control. Section 24.1(a) of LA FOIP 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;

[31] "Administrative safeguards" are controls that focus on internal organization policies, procedures, and maintenance of security measures that protect personal information. Examples include written policies and procedures, annual training for employees, confidentiality agreements, agreements with information management service providers (IMSPs), auditing programs, records retention and destruction schedules, and access restrictions (*Guide to FOIP*, Ch. 6, p. 89).

[32] In this case, SGI provided the following timeline of this privacy breach:

- Email with incorrect injury letter and blank forms attached was sent to a third party on Feb. 9/23.

- The third party reported the mistake to SGI on Feb. 22/23, and it was reported to PIM the same day.

- Investigation was opened on Feb. 22/23.

- PIM advised the manager LF on Feb. 23/23 that notification to the customer is necessary. RT advised her that she would provide her with wording for the letter.

- On Feb. 23/23 the complainant's blank documents were deleted from the third party's file.

- On Feb. 27/23, RT provided notification wording to LF so that she could create a letter to the complainant to be sent under her (LF's) name. LF sent the letter to the complainant the same day.

- In a discussion on April 18/23, LF advised RT that it was since determined that the blank documents were accidentally generated on the complainant's file instead of the third party's file, and then attached to the third party's file and sent to them.

[33] SGI also provided the following information:

> The PIR had more than one file open at the time of the mistake and generated the documents off the complainant's file instead of the third party's file; further, she did not check the attachment prior to sending the email.
>
> SGI staff are subject to a multitude of Corporate policies such as the Corporate Privacy Policy and the Code of Ethics and Conduct. Staff are required to annually sign off on a Confidentiality/Non- Disclosure Agreement, the Code of Ethics and Conduct and the Corporate Privacy Policy.
>
> Staff are regularly reminded to ensure that they are sending the correct information to the correct person. They are advised to double-check emails, addresses, letters, etc. prior to sending to ensure that all information is accurate and going to the correct person, and it appears that this did not happen in this case. Staff are fully aware that they have a duty to protect personal information.
>
> …Additionally, the privacy training SGI employees receive, both at commencement of employment and then annually, as well as the yearly policy signoffs reinforce this message.

[34] Based on SGI's response, it appears that the root cause of the privacy breach was administrative in nature, or the employee's failure to follow established procedures to ensure they send information to the correct person. Based on SGI's explanation and understanding of what occurred, I find that it conducted an adequate investigation. I will

assess how SGI intends to prevent similar breaches from occurring in the future in the next part of this Investigation Report.

Prevented future breaches

[35] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring.

- What steps can be taken to prevent a similar privacy breach.
    - 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.

(*Guide to FOIP*, Ch. 6, p. 274)

[36] SGI stated as follows:

> No changes to policies or procedures have been planned. As stated previously, staff are reminded regularly to ensure that they are sending the correct information to the correct person. They are asked to double-check emails, addresses, letters, etc. prior to sending to ensure that all information is accurate. This is regularly reinforced at staff meetings.
>
> … PIM also did a privacy presentation via Microsoft Teams to approximately 140 Injury Claims staff on April 13/23.

[37] While continuous reminders of policies and procedures are helpful, I also encourage SGI to explore ways in which it could proactively ensure that employees follow policies and procedures. Such measures could include randomly sampling or double checking how well employees are following policies and procedures. Based on SGI's response, I find that it has measures in place to prevent similar breaches from occurring, but that it could further explore ways to ensure employees follow policies and procedures.

III FINDINGS

[38] I find that I have jurisdiction to conduct this investigation.

[39] I find that the Complainant's personal information is involved pursuant to subsections 24(1)(a), (d), (e) and (k)(i) of FOIP.

[40] I find that a privacy breach occurred.

[41] I find that SGI took appropriate steps to contain the privacy breach.

[42] I find that SGI provided an adequate notification to the Complainant of the privacy breach.

[43] I find that SGI conducted an adequate investigation.

[44] I find that SGI has measures in place to prevent similar breaches from occurring, but that it could further explore ways to ensure employees follow policies and procedures.

IV RECOMMENDATION

[45] I recommend that SGI explore ways to ensure employees follow policies and procedures.

Dated at Regina, in the Province of Saskatchewan, this 26th day of October, 2023.

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