



Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 283-2021

Saskatchewan Telecommunications

September 6, 2022

Summary: Saskatchewan Telecommunications (SaskTel) notified the Complainant of a privacy breach involving their personal information. The Complainant followed-up with our office by submitting a breach of privacy complaint and requested that the Commissioner investigate the privacy breach. SaskTel proactively reported the matter prior to the Complainant contacting our office; however, as the email was caught in the spam filter, that was not acknowledged until after the fact. The Commissioner found that the Complainant's personal information was used without authorization and that a privacy breach occurred. The Commissioner found SaskTel took the appropriate steps to respond to this privacy breach and to prevent similar privacy breaches from occurring in the future. The Commissioner recommended that SaskTel take no further action.

I BACKGROUND

- [1] On November 9, 2021, the Complainant, an employee at Saskatchewan Telecommunications (SaskTel), received a text message from their manager requesting a telephone meeting. During the meeting, the Complainant was informed that a breach of privacy investigation was being conducted as a manager at SaskTel used their personal information without authority. On November 10, 2021, SaskTel followed-up with an email to the Complainant.
- [2] The breach occurred on October 22, 2021, when a manager (the Manager) saved an electronic copy of the Complainant's suspension letter to a SharePoint site that was accessible to internal SaskTel employees. On October 29, 2021, SaskTel removed the document from the SharePoint site.

- [3] On November 16, 2021, the Complainant asked my office to investigate the privacy breach.
- [4] On November 29, 2021, SaskTel contacted our office as it claimed to have proactively reported the matter to us on November 10, 2021, and had not heard back. Our office searched and confirmed that the email in question had been caught in our spam filter. As a complainant had already come forward, as noted in 4.6 of my office's [Rules of Procedure](#), even if proactively reported, the Commissioner may direct that a report will be issued where a person has filed a complaint with the Commissioner's office.
- [5] On December 3, 2021, my office notified SaskTel and the Complainant that it would be conducting a privacy breach investigation pursuant to section 33 of *The Freedom of Information and Protection of Privacy Act* (FOIP).

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

- [6] SaskTel is a "government institution" as defined at subsection 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP), and section 3 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 SaskTel respond appropriately to the privacy breach?

- [7] When reviewing if a public body has responded appropriately to a privacy breach, my office first determines if personal information is involved. If so, then my office considers if there was an unauthorized collection, use or disclosure of that personal information by the public body. If there has been, then my office moves on to assess whether the public body took the privacy breach seriously, and appropriately addressed it according to my office's [Rules of Procedure](#) (updated September, 2022).

[8] According to SaskTel’s submission, the unauthorized use of the Complainant’s personal information was related to their employment. SaskTel confirmed that an electronic copy of the Complainant’s suspension letter was accessible to employees of SaskTel. The suspension letter outlined that the Complainant was subject to discipline and included other details such as their home address. For clarity, in my office’s [Investigation Report 262-2018](#) at paragraph [9] of that report “employment history” means the type of information normally found in a personnel file such as performance reviews, evaluations and disciplinary actions taken, among other information.

[9] In determining whether personal information is involved, I refer to subsections 24(1) of FOIP, which contains a non-exhaustive list of information that constitutes personal information. Since the Complainant’s employment history, name and home address was listed, the following will apply:

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:

...

(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;

...

(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;

[10] I must note however that since the personal information was not shared with external parties outside of SaskTel, this data transaction is an unauthorized “use” and not a disclosure. As such, I will refer to this as an unauthorized use of the Complainant’s personal information.

[11] Based on this, the Complainant's personal information is involved in these matters. As SaskTel does not dispute that what occurred was unauthorized, I will move onto assessing if SaskTel appropriately addressed the privacy breach.

[12] In order to be satisfied that SaskTel appropriately addressed the privacy breach, my office will analyze the steps it took to address the breach. According to my office's resource, [*Privacy Breach Guidelines for Government Institutions and Local Authorities*](#) (*Privacy Breach Guidelines*), updated September 2021, and Part 4 of my office's [*Rules of Procedure*](#), I recommend four best practice steps in responding to a privacy breach:

1. Contained the breach (as soon as possible)
2. Notified affected individuals (as soon as possible)
3. Investigated the breach
4. Taken steps to prevent future breaches

(*Privacy Breach Guidelines*, pp. 4-7; *Rules of Procedure*, Part 4)

[13] I will now consider if SaskTel appropriately responded to this matter against these four best practice steps.

Contained the breach (as soon as possible)

[14] 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 was breached.
- Revoking access to personal information.

- Correcting weaknesses in physical security.

- [15] Effective and prompt containment reduces the magnitude of a breach and in some instances, the risks to an individual.
- [16] As previously mentioned, SaskTel confirmed that an electronic copy of the Complainant's suspension letter was inadvertently saved to an internal SharePoint site by a manager. This SharePoint site was accessible to all SaskTel employees.
- [17] On October 29, 2021, around 3:25 pm, an employee was browsing their Microsoft 365 documents landing page, which included the SharePoint site. While this employee was on the SharePoint site, they noticed a document that was not familiar to them. The employee accessed the document in question, and upon recognizing the personal nature of the document, reported it to a manager.
- [18] On October 29, 2021, at 3:30 pm, five minutes after it was reported, the document was removed from the SharePoint site by the SharePoint Administrator. At 4:18 pm the same day, the backups of the folder where the document was saved to, were deleted by the SharePoint Administrator. The Industrial Relations Team and the Human Resources Team checked the folders to ensure the document had been removed.
- [19] On November 4, 2021, logs from the SharePoint site were available and reviewed by the Security team, the Privacy team, and the Human Resources team to determine next steps. The logs confirmed which manager shared the document and which employees accessed it.
- [20] Between October 22, 2021, and October 29, 2021, a total of 14 employees were identified as having seen the suspension letter posted to the SharePoint site. Out of these 14, 11 of the employees saw the document link, but did not open the link. The remaining three employees clicked on the link and opened the document. Of these three employees, two of them admitted to viewing the information but closed the document once they realized the

personal nature of the letter. The third employee reported it to the Manager who posted the letter, resulting in the document being removed.

- [21] Human Resources completed interviews with all 14 employees on November 8, 2021, who were identified as having seen the document.
- [22] The logs were also used to determine whether the document was printed from the SharePoint site. According to the logs, none of the 14 individuals printed the document. Furthermore, all 14 employees were asked if any copies were produced via any other method (i.e. screen shots, pictures with a mobile device, etc.). The employees provided written confirmation that they had not made, retained, nor distributed any copies of the document containing the Complainant's personal information.
- [23] Based on the information provided, I find SaskTel took adequate steps to contain the privacy breach.

Notified affected individuals (as soon as possible)

- [24] Notifying an individual that their personal information and/or personal health 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 normally 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 breaches in the future.

- Steps to contact information of an individual within the organization who can answer questions and provide further information.
- A notice that the individuals have a right to complain to the Office of the Information and Privacy Commissioner.
- Recognition of the impacts of the breach on affected individuals and an apology.

[25] On November 9, 2021, as previously mentioned, the Complainant was notified via telephone by their Manager, the Privacy Consultant, and a Human Resources Manager that a breach of their personal information had taken place.

[26] On November 10, 2021, SaskTel's Regulatory Affairs Manager sent an email to the Complainant which included a description of what happened, what personal information was accessed, how many employees viewed the personal information, the findings of the investigation, what SaskTel has done to prevent similar incidents from occurring, an apology and my office's contact information. These are all elements that my office recommends a government institution include in a notification letter. SaskTel also notified the Complainant of the breach soon after it was discovered.

[27] Based on the preceding, I find that SaskTel provided appropriate notification.

Investigated the breach

[28] Investigating a privacy breach to identify the root cause(s) is key to understanding what happened and to prevent similar privacy breaches from occurring in the future. Below 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?

[29] SaskTel confirmed that suspension notice letter templates are sent from Industrial Relations to managers of employees to complete the relevant details. Once completed, the manager returns the letter electronically to Industrial Relations. It was during this process on October 22, 2021, that the Manager inadvertently saved the Complainant's suspension letter to the SharePoint site as opposed to the secure desktop location where it was intended to be saved to.

[30] The SharePoint site had open sharing permissions enabled as it was used for learning and development purposes. The open permission explains why the Manager was able to post it there and why employees were able to access the site's content. This resulted in the document being categorized as a shared document, and thus accessible to SaskTel employees.

[31] According to SaskTel's internal investigation report, documents of this nature are not typically sent back and forth, and managers do not have to complete suspension notice letters as a regular part of their job. SaskTel further reported there had been an increase in suspension letters, and due to this, the sharing process was changed. This process change failed to account for the increased risk involved in storing and saving confidential documents. SaskTel's investigation shows it recognized the contributing cause of this breach, then, was associated with the process flow of the documents.

[32] I find that SaskTel conducted an appropriate privacy breach investigation.

Taken steps to prevent future breaches

[33] An important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. 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.

[34] When considering what changes should be made, the public body can ask itself the following questions:

- 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?

[35] SaskTel reported to my office that it has implemented several changes to their process of sharing sensitive documents. The changes include the following:

1. The Industrial Relations team investigated an alternative process flow regarding letters containing personal information to limit the movement of sensitive documents, thereby reducing the likelihood of documents being shared inadvertently.
2. The Industrial Relations team now includes direct and specific instructions to managers detailing steps to edit sensitive documents as necessary, but not to keep or store the document anywhere other than approved and secure locations.
3. The Manager who shared the document completed privacy training and SharePoint training on November 26, 2021.
4. SaskTel's Human Resources Manager reviewed the Manager's electronic devices for any additional copies of the letter and explained the saving and sharing process.

[36] SaskTel also included the following safeguards, which they have implemented:

Administrative controls:

- Employee Privacy Policy
- Employee Privacy Training
- Privacy Impact Assessments
- Letters have a statement on them indicating they are private and confidential.

Technical Controls:

- Site was restricted to specific internal employees including managers requiring log-in to access.
- When saving documents, there are other locations that are prompted as locations that can be used. This includes, but is not limited to, secure storage for individual employee's use.

Physical Controls:

- The Industrial Relations team has a locked door, only employees in that area can enter.
- The entire company has security personnel ensuring access to the buildings is granted only to authorized employees (who would also then require a log in to a system to access the document).
- There is a template of the letter that is shared only when necessary.

[37] Given what SaskTel has outlined, I find that it has taken appropriate steps to prevent similar privacy breaches from occurring in the future.

III FINDINGS

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

[39] I find that SaskTel took appropriate steps to contain the privacy breach.

[40] I find SaskTel provided appropriate notification to the Complainant.

[41] I find SaskTel investigated the privacy breach and identified the root causes.

[42] I find SaskTel took appropriate steps to prevent a similar privacy breach from occurring in the future.

IV RECOMMENDATION

[43] I recommend that SaskTel take no further action.

Dated at Regina, in the Province of Saskatchewan, this 6th day of September, 2022.

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