Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 032-2024, 097-2024

Saskatoon Police Service

August 27, 2024

Summary: The Saskatoon Police Service (SPS) had identified that three of its sworn members had snooped on personal information stored within its records management system (RMS) for personal, non-business-related reasons. SPS proactively reported the privacy breaches to my office as well as notified the affected individuals. One of the affected individuals requested that the A/Commissioner conduct an investigation into the matter. The A/Commissioner made a number of findings, including that privacy breaches occurred, that the SPS took steps to contain and investigate the breaches and that SPS is taking reasonable steps to minimize the likelihood of similar privacy breaches from occurring in the future. However, the A/Commissioner also recommended that SPS further investigate details of actions taken by one of the sworn members and to report its findings to his office within 30 days of issuance of this Investigation Report.

I BACKGROUND

[1] On October 17, 2023, a Superintendent at the Saskatoon Police Service (SPS) requested that SPS's Access and Privacy Unit conduct an audit to determine if there had been any inappropriate accesses to a particular investigation file in SPS' records management system "RMS". The audit revealed that one sworn member of the SPS (Sworn Member A) had accessed the personal information of five individuals inappropriately. The audit also revealed that Sworn Member A had queried certain addresses as well as four individuals linked to those particular addresses. Sworn Member A had used their own login credentials into RMS to conduct the queries. Additionally, it was discovered that Sworn Member A had accessed the RMS using another member's credentials when the other member was away from their computer, to conduct further queries and print pages from a specific file.

[2] On October 26, 2023, the Deputy Chief of Operations directed the Professional Standards Division (PSD) to conduct an investigation into whether Sworn Member A accessed information into an investigation for a non-business purpose. Through that investigation, SPS determined that two other sworn members (Sworn Member B and Sworn Member C) had accessed the personal information of a particular individual inappropriately.

[3] On February 14, 2024, SPS proactively reported the privacy breach to my office.

[4] In letters dated February 29, 2024, SPS notified the affected individuals that their personal information had been inappropriately accessed.

[5] On March 8, 2024, my office notified the SPS that my office would be undertaking an investigation (file 032-2024).

[6] On March 19, 2024, one of the affected individuals (Complainant) requested that my office conduct an investigation into this matter.

[7] On April 3, 2024, my office notified both the SPS and the Complainant that my office would be undertaking an investigation (097-2024).

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[8] SPS qualifies as a "local authority" as defined by subsection 2(1)(f)(viii.1) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). Therefore, I find that I have jurisdiction to conduct this investigation.

2. Did privacy breaches occur?

[9] A privacy breach occurs where there is an unauthorized collection, use and/or disclosure of personal information (*Guide to LA FOIP*, Chapter 6: "Protection of Privacy", updated February 27, 2023 [*Guide to LA FOIP*, Ch. 6], p. 234). First, I must determine if "personal information" is involved. Then, I must determine if the personal information is in the possession or under the control of SPS. If so, then I must determine if there was authority under LA FOIP for Sworn Members A, B, and C to have accessed the personal information.

a. Is personal information involved?

[10] For Part IV of LA FOIP to be engaged, there must be personal information as defined by subsection 23(1) of LA FOIP. In this case, subsections 23(1)(a), (b), (d), (e), (f), (h) and (k) of LA FOIP are relevant:

> **23**(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;
>
> (e) the home or business address, home or business telephone number, fingerprints or blood type of the individual;
>
> (f) the personal opinions or views of the individual except where they are about another individual;
>
> ...
> (h) the views or opinions of another individual with respect to 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.

[11] Sworn Members A, B and C had accessed individuals' personal information in SPS's RMS system. In its submission, SPS said the following:

> The following types of personal information was involved in this breach:
>
> - General identifying information such as name, date of birth, home address, phone number;
> - Information relating to criminal history and police involvement, including details of police investigations involving the affected individuals;
> - Identifying number such as license plate number*;
>   - Generally, license plate numbers are not considered personal information, however in this case the SPS considers this information personal in nature, as [Sworn Member B]'s query of a license plate in order to identify a vehicle owner was not for a business purpose;
> - Opinions of others about identifiable individuals; and
> - The name of individuals where it appears within police records.
>
> This information is considered personal information as per subsections 23(1)(a),(b),(d),(e),(f),(h), and (k)(i) of LA FOIP,…

[12] Based on the above, I find that personal information is involved as defined by subsections 23(1)(a), (b), (d), (e), (f), (h) and (k) of LA FOIP.

b. Is personal information in the possession or under the control of SPS?

[13] Earlier, I noted that the personal information was stored in SPS's RMS. Therefore, I find that the personal information is in the possession and under the control of SPS.

c. Was there authority under LA FOIP for Sworn Members A, B and C to have accessed the personal information of the affected individuals?

[14] "Use" means the internal utilization of personal information by a local authority and includes the sharing of the personal information in such a way that it remains under the control of the local authority (*Guide to LA FOIP*, Ch. 6, p. 152). Therefore, when sworn

members of the SPS accesses personal information stored within RMS, those accesses would be considered a "use" of personal information.

[15] A local authority must only use personal information in accordance with section 27 of LA FOIP. Section 27 of LA FOIP provides:

> **27** No local authority shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:
>
> (a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or
>
> (b) for a purpose for which the information may be disclosed to the local authority pursuant to subsection 28(2).

[16] In SPS' Access and Privacy Unit's investigation report, SPS noted that the accesses to personal information within the RMS was for reasons that were personal and unrelated to their work. The "need-to-know" principle states that information should only be available to those in an organization who need to know it for purposes related to their immediate duties (*Guide to LA FOIP*, Ch. 6, p. 23). Therefore, there was no authority under LA FOIP for Sworn Members A, B and C to have accessed the personal information in RMS. I find that privacy breaches occurred.

3. Did SPS respond appropriately to the privacy breach?

[17] My office's *Guide to LA FOIP*, Ch. 6 at page 236, suggests that local authorities use the following four steps to respond to a privacy breach:

- Contain the breach.
- Notify affected individuals.
- Investigate the breach.
- Prevent future breaches.

[18] I will consider these four steps to determine if SPS responded appropriately to the privacy breach.

Contain the breach

[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 LA FOIP*, Ch. 6, p. 236)

a. Sworn Member A

[20] When SPS discovered that Sworn Member A had inappropriately accessed personal information in the RMS, Sworn Member A was no longer assigned to the unit they were in when the inappropriate access occurred, and required access to the RMS to conduct their duties. Therefore, the SPS closely monitored and audited their access to the RMS. Once access was no longer required for their regular duties, Sworn Member A's access to the RMS was revoked. SPS has informed my office that Sworn Member A does not have access to the RMS and there is no timeline as to when they will be provided access.

[21] Regarding the printed records, SPS said in its investigation that Sworn Member A said they destroyed the records and did not disclose the information to anyone. My office sought additional information from SPS – such as where did Sworn Member A take the printed records? Who destroyed the records and when? In what manner were the records destroyed? Further, my office asked if Sworn Member A provided a written confirmation

that they did not disclose the information they queried to any other person. However, SPS was unable to provide my office with such information.

[22] I find that SPS should take additional steps to contain the privacy breach committed by Sworn Member A.

[23] Therefore, I recommend that SPS investigate the following and provide my office with its findings within 30 days of issuance of this Investigation Report:

- Where did Sworn Member A take the printed records?
- Who destroyed the records and when?
- In what manner were the records destroyed?

[24] If SPS complies with my above recommendation and provides my office with its findings, my office may open another investigation into the matter if my office determines that SPS has not taken steps to sufficiently contain the personal information breached in this matter.

[25] As well, I recommend that SPS seek written confirmation from Sworn Member A that they did not disclose the information they queried to any other person and provide my office with a copy of the written confirmation within 30 days of issuance of this Investigation Report.

b. Sworn Members B and C

[26] SPS said in its Access and Privacy Unit's investigation report that they audited Sworn Members B and C and found they had made no further suspicious queries. As such, SPS did not revoke their access to the RMS. SPS continues to audit their access to the RMS and it has not found any non-business-related queries. I find that SPS has taken steps to contain the privacy breaches committed by Sworn Members B and C.

[27] I recommend that SPS seek written confirmation from Sworn Members B and C that they did not disclose the information they queried to any other person and provide my office

with a copy of the written confirmations within 30 days of issuance of this Investigation Report.

Notify affected individuals

[28] Local authorities should notify individuals affected by the privacy breach as soon as possible after key facts about the breach have been established. My office's *Guide to LA FOIP*, Ch. 6 at pages 237-238, outlines that notices to affected individuals 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 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 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.

[29] In total, there were nine affected individuals. SPS sent registered letters to seven of the nine affected individuals containing the above elements. Letters to one of the seven individuals was returned to the SPS as unclaimed. Therefore, SPS was able to obtain the email address for this one specific individual and forwarded the letter via email.

[30] Regarding the two individuals who were not notified, SPS said it did not have updated contact information for them, so they were unable to send letters to notify them of the privacy breach.

[31] Based on the above, I find that SPS has made a reasonable effort to notify the individuals affected by the privacy breach.

Investigate the breach

[32] Once a breach has been contained, the next step is to investigate the breach. This step includes identifying the root cause of the privacy breach (*Guide to LA FOIP*, Ch. 6, pp. 238-240).

[33] SPS indicated to my office that it requires all staff to complete a LA FOIP Training Module bi-annually. Further, SPS said that it provided LA FOIP training to all of its employees in early 2017 before SPS became subject to LA FOIP. Then, SPS made LA FOIP training mandatory for all members in 2018, 2020 and 2022. Further, all new SPS employees receive LA FOIP training. SPS provided my office with copies of its policies and resources, including its LA FOIP Intranet Information Sheet. This information sheet says:

> **Access and use personal information for business purposes only (Need to know)** – You may only access SIMS [now known as RMS] and other SPS databases in the performance of your duties. Systems access is audited, so you will be held accountable for accessing information outside the performance of your duties.

[34] Finally, upon logging into the RMS, a pop-up message appears. The message contains a sentence that explicitly says, "Access for personal reasons is prohibited". Staff are not able to proceed further into the system until they select "OK".

[35] In its Access and Privacy Unit's investigation report, SPS said that the three sworn members…

> …knew, or ought to have known, that access to the personal information identified was not for a business purpose, and was therefore inappropriate and a contravention of SPS policy and LA FOIP. The SPS does not believe that the breach occurred due to a lack of reasonable security measures on the part of the SPS, but by the wilful decisions of the subject employees.

[36] SPS noted that it was personal reasons that Sworn Members A, B and C inappropriately accessed personal information in the RMS. Based on the identities of the individuals

snooped upon, it is evident to my office that Sworn Members A, B and C accessed the personal information for personal reasons and not work-related reasons. I agree with SPS' finding that the three sworn members inappropriately accessed information based on their own wilful decisions. I find that the root cause of the privacy breaches is that the sworn members disregarded policy and the pop-up message on the RMS prohibiting access for personal reasons.

Prevent future breaches

[37] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring (*Guide to LA FOIP*, Ch. 6, p. 243). In its Access and Privacy Unit's investigation report, SPS indicated the following:

- Potential discipline
- Logging off feature
- Training
- Auditing

a. Potential Discipline

[38] In its Access and Privacy Unit's investigation report, SPS indicated this matter has been referred for potential discipline under *The Police Act, 1990*. SPS said the following:

> The investigation into the actions of the noted members was deemed an internal matter, and is therefore guided by section 54(1) of the Police Act, which provides:
>
> > **54**(1) A chief shall cause an investigation to be conducted into any allegation of misconduct by a member, including an allegation that the actions of the member may constitute an offence pursuant to an Act or an Act of the Parliament of Canada.
>
> If any of the allegations against the members are found to be substantiated, the members may be subject to disciplinary action as per *The Municipal Police Discipline Regulations, 1991*.

[39] My office sought an update on whether the three sworn members had been disciplined. SPS indicated that the "matter is still ongoing".

b. Logging off feature

[40] Sworn Member A was able to use another sworn member's credentials to conduct queries in RMS when the other sworn member vacated the computer without logging off. Therefore, SPS said it was reviewing an automatic log off feature for computers. Further, it is reviewing the potential for staff to be required to enter a reason upon making a query in RMS.

[41] In addition to the automatic log off feature it is reviewing, I recommend that SPS ensure that it provides training and reminders to its employees to log off RMS and any other application before vacating a computer.

c. Training

[42] SPS said it was requiring all SPS staff to re-take its mandatory LA FOIP module training by June 30, 2024. SPS advised my office that there was a 79% completion rate for all employees (which includes employees who are away on leave). SPS' Access and Privacy Unit indicated that it would be contacting its Human Resources Director requesting that employees who have not completed the training this year to receive a follow-up. I recommend that SPS take action to ensure all its employees complete the LA FOIP module training by the end of the calendar year, and that SPS require its employees to re-take the training annually. If employees are on leave, then I recommend that SPS require employees to complete the LA FOIP module training upon their return.

d. Auditing

[43] SPS indicated that it is auditing accesses by all three sworn members on a monthly basis. It is also conducting audits of general access to the RMS by all SPS employees in relation

to the affected individuals in this case. SPS reports it has not identified any non-business-related queries.

[44] Also, SPS noted it has an automated auditing system that flags certain queries in the system as suspicious. For example, when a user queries a person with the same last name or when they query an employee's name. If either occurs, then the Access and Privacy Officer is prompted to conduct a more in-depth review of an employee's access. In the course of my office's investigation, the SPS said this automated auditing system is relatively new, so it does not have specific policies or procedures for it yet. SPS said it would develop a procedure regarding this automated auditing system.

[45] I find that SPS is taking reasonable steps to minimize the likelihood of similar privacy breaches in the future.

III FINDINGS

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

[47] I find that a privacy breach occurred.

[48] I find that SPS should take additional steps to contain the privacy breach committed by Sworn Member A.

[49] I find that SPS has taken reasonable steps to contain the privacy breaches committed by Sworn Members B and C.

[50] I find that SPS has made a reasonable effort to notify the individuals affected by the privacy breach.

[51] I find that the root cause of the privacy breaches is that the sworn members disregarded policy and the pop-up message on the RMS prohibiting access for personal reasons.

[52] I find that SPS is taking reasonable steps to minimize the likelihood of similar privacy breaches in the future.

IV RECOMMENDATIONS

[53] I recommend that SPS investigate the following and provide my office with its findings within 30 days of issuance of this Investigation Report:

- Where did Sworn Member A take the printed records?
- Who destroyed the records and when?
- In what manner were the records destroyed?

[54] I recommend that SPS seek written confirmation from Sworn Member A that they did not disclose the information they queried to any other person and provide my office with a copy of the written confirmation within 30 days of issuance of this Investigation Report.

[55] I recommend that SPS seek written confirmation from Sworn Members B and C that they did not disclose the information they queried to any other person and provide my office with a copy of the written confirmations within 30 days of issuance of this Investigation Report.

[56] I recommend that SPS ensure that it provides training and reminders to its employees to log off RMS and any other application before vacating a computer.

[57] I recommend that SPS take action to ensure all its employees complete the LA FOIP module training by the end of the calendar year, and that SPS require its employees to re-take the training annually. If employees are on leave, then I recommend that SPS require employees to complete the LA FOIP module training upon their return.

Dated at Regina, in the Province of Saskatchewan, this 28th day of August, 2024.

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