Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 153-2022, 164-2022, 168-2022, 169-2022, 170-2022, 195-2022

City of Saskatoon

January 23, 2023

Summary: The City of Saskatoon (City) proactively reported a privacy breach to the Commissioner. The City had left boxes containing labour relations records, some which contained personal information, in an unlocked room. The City notified affected individuals of what had occurred; as a result, five individuals made a complaint to the Commissioner. The Commissioner found a privacy breach occurred, and so assessed the City's response to the breach. The Commissioner found the City could have taken additional steps to contain the breach, that it provided adequate notice, that it undertook an adequate investigation, and that it has an adequate prevention plan. The Commissioner recommended that in the future, the City request individuals who knowingly or unknowingly viewed personal information, without authority, of their responsibility to not retain or further disseminate the information. The Commissioner also recommended the City ensures all its employees and contractors complete the City's online access and privacy training on an annual basis.

I BACKGROUND

[1] On August 19, 2022, the City of Saskatoon (City) contacted my office stating, "the City of Saskatoon is proactively reporting a privacy breach involving physical labour relations records" (IPC File 153-2022).

[2] On August 23, 2022, my office provided notification to the City regarding my office's intention to undertake an investigation.

[3] On September 1, 2022, my office notified the City that my office had received four complaints regarding the alleged breach (IPC files 164-2022, 168-2022, 169-2022, 170-2022, 195-2022). On October 12, 2022, my office notified the City of a fifth complaint (IPC file 195-2022). My office added that, as a result of the complaints, my office would be issuing this Investigation Report.

[4] On September 23, 2022, the City provided my office its completed "Privacy Breach Questionnaire", internal investigation report and materials. The Complainants did not provide formal submissions.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[5] The City qualifies as a "local authority" pursuant to subsection 2(f)(i) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). Therefore, I have jurisdiction to undertake this investigation.

2. Did a privacy breach occur?

[6] The City notified affected individuals that the following data elements were contained in the records:

> The personal information in the unattended hard-copy paper records included your name and one or more of the following types of personal information: contact information, employee ID number, date of birth, income data, demographic data, health history, documents related to the course of your employment, face picture, and/or your signature.

[7] These data elements can be defined as "personal information" pursuant to subsections 23(1)(a), (b), (c), (d), (e) and (j) of LA FOIP, which provide as follows:

> **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;
>
> (c) information that relates to health care that has been received by the individual or to the health history of the individual;
>
> (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;
>
> …
> (j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or

[8] Once it is established that personal information is involved, the next step is to consider if a privacy breach occurred. In this matter, the City does not dispute that one did occur. I will nonetheless consider the events that transpired, which the City summarized as follows:

> Between June 20, 2022 and July 11, 2022, twenty-six (26) full or partially filled banker boxes containing confidential and non-confidential labour relations information as well as personal information as defined by The Local Authority Freedom of Information and Protection of Privacy Act, were moved from a secure storage location at Civic Square East (CSE) to an unsecured boardroom [redacted] in the same CSE building due to a water leak.
>
> Labour Relations (LR) was aware that the boxes were missing as early as July 5, 2022. Nonetheless, the privacy breach was discovered by the Corporate Records Manager while attending a meeting in that boardroom on July 11, 2022.
>
> …
> This was not an authorized disclosure. All in all, the City cannot say with high degree of assurance who actually accessed or could have accessed the personal information, if anyone. It is only known how long the personal information was exposed to improper disclosure.

[9] The City added it was moving its Labour Relations staff (and the records) back to City Hall from their Civic Square East (CSE) location. When staff moved back to City Hall, the records initially stayed behind at CSE and were moved to a couple different secure

locations within CSE. After it converted the second location to an office, the City relocated the records within CSE to a storage room. According to the facilities manager, the City issued 53 keys to City employees and contractors who had access to the storage room.

[10] On June 20, 2022, there was a water leak at CSE that could have damaged the boxes of records. The building operator then asked a plumber to move them. Because of the number of boxes, the plumber asked a carpenter to assist. While the records should have been moved to protect them from damage, none of these individuals was authorized to undertake the move on their own. Nonetheless, the floor where the plumber moved the records housed a different City department. While that floor had secure access (i.e., only employees of that department and limited contractors had access), the records were placed in an unlocked boardroom. Employees on that floor sometimes used the boardroom to make private, personal calls. Labour Relations found out about the move on July 5, 2022, when it inquired with the facilities manager about the boxes of records. Between June 20 and July 5, it appears Labour Relations lost track of the records.

[11] In my office's Investigation Report H-2011-001 concerning Dr. Teik Im Ooi, medical records had been moved around and left unsecured for a number of years in a Regina strip mall. While there was no proof anyone had viewed or taken any records during the movement of the records, the fact that they had been left unsupervised for extended periods of time greatly increased the probability of that occurring.

[12] This matter is similar as the City's Labour Relations department was not aware the records had been moved to an unlocked boardroom for a number of weeks. The move was not supervised or conducted by authorized personnel, and the records were left in a place where individuals, whether by accident or not, may have viewed or taken some of the records. Some of the personal information in the records or data elements were quite sensitive in nature and could be misused for fraudulent purposes. I add that the City did not state whether it had logged the records prior to storing them to later determine if any were missing - logging records that are being moved is helpful in assessing containment if a privacy breach later occurs.

[13] Section 23.1 of LA FOIP outlines the duty of a local authority to protect personal information in its possession or under its control as follows:

> **23.1** Subject to the regulations, a local authority 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;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[14] For a number of reasons, the City did not adequately protect the personal information in its possession or under its control pursuant to subsection 23.1 of LA FOIP. Because of this, there were many possibilities for a privacy breach to have occurred, and so I find that one did. My next step is to assess how the City managed the breach.

3. Did the City respond appropriately to the breach?

[15] My office's *Rules of Procedure* outlines that my office will analyze whether the government institution properly managed the breach and took the following steps in responding:

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

[16] I will consider each step separately and make any necessary recommendations at the end of this Investigation Report.

Contained the breach (as soon as possible)

[17] Upon learning that a privacy breach has occurred, steps should be taken to immediately 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; and
- Correcting weaknesses in physical security.

(*Privacy Breach Guidelines*, p. 4)

[18] In terms of containment, the City stated as follows:

> Considering all of these factors, including the nature of the information involved, Labour Relations failed in their effort to:
>
> 1) Failed to protect the personal information in its custody or control.
>
> 2) Report the privacy breach following the initial determination that the records were missing (definition of a privacy breach, responsibility for managing a breach, and steps to reporting any breach or suspected breach, are codified within the recently modified 'Administrative Procedure: CK-002 Title: Privacy Breach' available on SharePoint (last updated on 2022-05-30)).
>
> 3) Prioritize the containment of the breach resulting in excessive delays in locating and securing the misplaced records.

[19] The City added the following:

> Labour Relations (LR) was aware that the boxes were missing as early as July 5, 2022. Nonetheless, the privacy breach was discovered by the Corporate Records Manager while attending a meeting in that boardroom on July 11, 2022.

> The Corporate Records Manager promptly reported the unattended boxes to the Deputy City Clerk – Records, Information, Access & Privacy Services. Based on discussion with the Deputy City Clerk, the boxes were brought to City Hall under the direction of the Corporate Records Manager and Security to be locked securely in the Labour Relations office at City Hall.

[20] The City added that within one hour of the Corporate Records Manager noticing the records sitting unattended, they had them moved to a secured location. At that point, the City considered the records to be contained. The purpose of containing a breach right away is to ensure a privacy breach does not continue. By moving the records to a secure location, the City did effectively contain the situation.

[21] Previously in this Investigation Report, I mentioned that the City did not state if it had prepared a list of the records it was moving. If it had, it would have been able to cross-reference records being moved from storage to their new location. While no public body would anticipate a privacy breach occurring, a best practice is to prepare a list of records going for storage so that you can account for them later, particularly if containment becomes an issue (see Investigation Report 145-2022 and Investigation Report H-2011-001).

[22] As I also previously explained, there were possibilities regarding who could have accessed the records without authority. This also affects the ability to contain a breach. If you do not know for certain that certain records could have been viewed – or even taken – then you do not have full containment. A step the City should have taken was to contact (e.g., through email) any City employees and contractors who would have had access to the records during the time in question and: 1) ask if any did access or take records; and 2) advise them of their obligations to return or not disclose or disseminate any information they may have knowingly or unknowingly accessed. This step would have further helped the City's containment efforts.

[23] While the City did take immediate steps to contain the records, I find it could have taken some additional steps to ensure adequate containment.

Notified affected individuals (as soon as possible)

[24] It is a best practice to inform affected individuals and my office of a privacy breach. The following is a list of individual organizations that may need to be notified as soon as possible after learning of the incident:

- The organization's privacy officer
- My office
- The police, if criminal activity is suspected and
- The affected individual(s) (unless there are compelling reasons why this should not occur).

(*Privacy Breach Guidelines*, pp. 4 to 5)

[25] Providing notice to individuals affected by the breach should occur as soon as possible after key facts about the breach have been established. In terms of notification, my office's *Privacy Breach Guidelines* offers the following guidance at page 4:

> 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.

[26] Besides my office, the City also notified its legal counsel, corresponding unions and boards, the mayor and council, and its media relations manager. These were all positive steps to take.

[27] The City further mailed registered letters to affected individuals to notify them of the breach. All letters contained information on what had occurred, steps the City was taking to address the breach, and the option for affected individuals to make a complaint to my office. These are all elements I look for in a notice to individuals.

[28] The City sent a different type of letter depending on one of three assessed levels of risk to the individual. The City assessed the risk based on the data elements contained in the record. These levels included, "Medium Risk Mailing", "High Risk Offer Mailing", and "High Risk List". The City's internal investigation report indicates that it provided one year of identity theft monitoring to 347 individuals assessed as "high" risk. The City added that it took into consideration that high-risk files contained data elements such as social insurance and health card numbers, driver's license information and fingerprints. These types of data elements can certainly place an individual at a higher risk for identity theft. I commend the City for taking this step.

[29] The City added it took it 43 days from the time the breach was known to send out its notification letters. The City stated it wanted to take time to ensure it had correct information for each individual, and to avoid duplicate letters being sent. While 43 days is not necessarily timely, I recognize the City took steps to ensure it had proper contact information.

[30] Given all this, I find the City's notification efforts were adequate.

Investigated the breach

[31] When considering why a privacy breach occurred, a trustee should reflect on the root causes, or what led to the breach occurring. It is an important step in mitigating the risk of a future breach of a similar nature from occurring. Following 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?

(*Privacy Breach Guidelines,* pp. 6 to 7*)*

[32] The City stated the root cause as follows:

> This root cause of privacy breach was non-compliance with the City's record-keeping requirements, and human error with regards to the loss of visibility and physical control over the files.
>
> The following expectation under the Corporate Records and Information Management Policy were not met:
>
> 4.1. All records, regardless of media, must be retained and disposed of in accordance with Records Retention and Disposal Schedules established by City Council as required by The Cities Act. Records will only be kept longer than their scheduled disposition if they are involved in litigation or audit.
>
> 4.3 All records must be maintained in accordance with practices and procedures set out in the Records and Information Management Procedures document.
>
> 4.4 Records containing personal information must be maintained in such a manner to protect the privacy of the individual(s) and to provide access to information as provided for under The Local Authority Freedom of Information and Protection of Privacy Act.
>
> 4.6 All records in printed form will be physically stored in the Corporate standard filing equipment and containers approved under the Records and Information Management program, as specified in the Records and Information Management Procedures.
>
> 4.8 Inactive records must be stored at the approved off-site location (commercial records centre). To provide for appropriate security of records, only employees authorized by the Department or Branch Manager and the Corporate Records Manager will have access to forward for storage and retrieve records from the off-site records centre. Access will be restricted to two employees per filing system.

[33] The City provided my office with copies of its administrative and record keeping policies and procedures, as well as links to online privacy materials and "E-learning Courses" for managers, supervisors and directors. These resources describe policies and procedures for such topics as access to information, and storage and retention of personal information. These appear to be adequate resources and appear accessible to City employees.

[34] The City also listed the individuals it interviewed during the course of its investigation. This included the facilities manager, the manager of the area where the records had been moved to avoid water damage, the plumber who moved them, and personnel within human resources. It appears the City interviewed anyone who had responsibility for, or who came in contact with, the records; these would be appropriate individuals to interview in the given circumstances.

[35] Based on what the City has provided, I agree that the root cause was a failure to follow established administrative safeguards. 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 (*Privacy Breach Guidelines*, p. 2).

[36] I add that there was also a failure to ensure proper physical safeguards. These are the physical measures, policies, and procedures to protect personal information and related buildings and equipment from unauthorized intrusion and natural and environmental hazards. Examples include locked filing cabinets, offices and storage rooms, alarm systems, and clean desk approaches (*Privacy Breach Guidelines*, p. 2). This occurred when the records were left in a room that was not locked or monitored.

[37] The City recognizes and accepts responsibility for the errors that occurred. Based on its identification of the root cause, I find the City conducted an adequate investigation.

Prevented future breaches

[38] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. Essentially, what steps can be taken to prevent a similar privacy breach from occurring? To assist, some questions trustees can ask are:

- 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?

(*Privacy Breach Guidelines*, p. 7)

[39] The City outlined its list of actions as follows:

- Completed by: All Labour Relations personnel and Interviewees (EG plumber, corporate security)

  Completion Date: December 31, 2022

  Recommendation #2: Completion of records management training via LMS. Proof of completion (course completion certificate) should be provided to the Privacy Officer to close this action item

- Completed by: All Labour Relations personnel

  Completion Date: December 31, 2022

  Recommendation #3: Work with the Records and Information Management Coordinator to relocate the 26 boxes from vulnerable workplace storage rooms and self-storage units into the secure offsite facility in accordance with the City's policies and procedures

- Completed by: All Labour Relations personnel, HR RIM Coordinator(s)

  Completion Date: December 31, 2022

  Recommendation #4: Work with the Records and Information Management Coordinator to create an organized work environment for controlling documents and records from piling up in boxes. This includes: a) eliminating unnecessary over-retention of unsecured/secured files b) strengthening the tracking and monitoring practices for any physical record transfers that are made c) moving to digital document management (EG the use of Documentum)

- Completed by: All Labour Relations personnel, HR RIM Coordinator(s)

  Completion Date: December 31, 2022

Recommendation #5: Create and execute a plan to transition from paper-based records to electronic records - electronic records require less space and fewer administrative resources to maintain and are generally easier to read and locate than paper-based records which are handwritten, incomplete and dispersed across various locations; electronic records can also be designed to enhance the privacy of individuals and the security of personal information through safeguards such as access controls, logging, and auditing functionality

- Completed by: Chief Human Resource Officer, Director, Labour Relations

  Completion Date: December 31, 2023

  Recommendation #6: Sharing of the lessons learned from this breach matter during departmental and Senior Management Team meeting

- Completed by: Director, Labour Relations, and Deputy City Clerk

  Completion Date: December 31, 2022

  Recommendation #7: Completion of a physical walkthrough of all HR related areas identifying potential privacy (or security) gaps which represent real opportunities for breaches and to make the necessary corrections to eliminate or reduce the risk exposure

- Completed by: Manager, Labour Relations, Manager, Human Resources Business Partners

  Completion Date: December 31, 2023

  Recommendation #8: Allocate funding for a dedicated staff resource to establish an effective document management strategy and to support HR's processes and efforts in employee records and information management including transitioning to "less paper"

- Completed by: Chief Human Resource Officer, Director, Labour Relations

  Completion Date: 2023

  Budget – Approx. November

[40] In follow up to the recommended actions, the City noted some of the following highlights (which I am paraphrasing):

- The City received "91 follow up emails or phone calls from affected individuals seeking further information…". The City added that as of November 4, 2022, only one of these files remains open. The City also received 16 requests for file destruction from individuals, and have carried through with only one request left open as of November 4, 2022. The City was also able to identify individuals whose addresses required updating.

- All Labour Relations staff completed online privacy breach training, and some have completed or will complete records management training.
- The City will maintain the records in a secure location until its investigation is complete. This secure location will allow the records in question to be more easily accessed if there are requests from affected individuals. This will also allow the City to manage the further storage or destruction of records, as necessary.
- The City expects work towards digital filing for all its Human Resources division to take one to two years. A proposal has been drafted that outlines the objectives.
- Lessons learned will be presented to the Senior Management team.
- There will be a physical audit of the Human Resources area to identify security gaps and recommend corrective actions.

[41] One thing I note is that the City did not state if anyone who possibly had access to the records (e.g., the 53 aforementioned keyholders to the secure storage room, or the employees from the different department) had received prior access and privacy training, or had signed an oath of confidentiality. If not, these are steps that should have occurred, or safeguards the City should be mindful of in its assessment of the breach and its prevention plan.

[42] Based on what the City has identified about what it has already done, and what it intends to do, I find it has an adequate plan for prevention.

III FINDINGS

[43] I find I have jurisdiction to conduct an investigation.

[44] I find a breach occurred.

[45] I find the City could have taken some additional steps to contain the breach.

[46] I find the City provided adequate notice.

[47] I find the City conducted an adequate investigation.

[48] I find the City has an adequate plan for prevention.

IV RECOMMENDATIONS

[49] I recommend that, in the future, the City requests individuals who may have knowingly or unknowingly viewed or taken personal information, without authority, of their responsibility to return it, or to not disclose or further disseminate it.

[50] If it does not already do so, I recommend the City ensures all its employees and contractors complete the City's online access and privacy training on an annual basis.

Dated at Regina, in the Province of Saskatchewan, this 23rd day of January, 2023.

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