Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 299-2017

Saskatchewan Legal Aid Commission

January 18, 2018

Summary: Saskatchewan Legal Aid Commission (SLAC) reported a privacy breach to the Information and Privacy Commissioner (IPC) when a client file went missing. The IPC made a few recommendations, including how SLAC should make it a regular practice to identify threats to the protection of personal information and it identify appropriate safeguards to protect against those threats.

I BACKGROUND

[1] On November 22, 2017, a lawyer from Saskatchewan Legal Aid Commission (SLAC) was at the Battlefords Courthouse to speak to five or six files in court. The lawyer had placed the client files on a defence counsel table. Then, from 11:00am to 11:20am, the lawyer had stepped into the hallway to speak to two of his clients. When he returned, he discovered that one of the client files – which was in a blue folder - had gone missing.

[2] The next day, on November 23, 2017, SLAC proactively reported this privacy breach to my office.

II DISCUSSION OF THE ISSUES

[3] SLAC is a "government institution" as defined by subsection 2(1)(d)(ii)(A) 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*.

1. Was the duty to protect pursuant to subsection 24.1 of FOIP fulfilled?

[4] Prior to January 1, 2018, my office's position was that government institutions had an implied duty to protect personal information. As of January 1, 2018, the duty has now been enshrined in statute. Subsection 24.1 of FOIP imposes a duty upon government institutions to protect personal information. Specifically, subsection 24.1(b)(ii) of FOIP provides that government institutions must establish policies and procedures to maintain administrative, technical and physical safeguards that protect against any reasonably anticipated loss of personal information in its possession or under its control. Subsection 24.1 of FOIP provides as follows:

> 24.1 Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> ...
>
> (b) protect against any reasonably anticipated:
>
> ...
>
> (ii) loss of the personal information in its possession or under its control;

[5] SLAC's *Client Information Management Policy* provides guidance on how personal information is to be managed outside of the office and specifically within a court room. It says:

> 2. OUTSIDE THE OFFICE
>
> Personal information can be more easily lost or compromised when outside of the office. The following guidelines are expected to be followed when transporting files, diaries, computers or cell phones or having them at other locations. Documents are expected to be returned to the Area Office as soon as reasonably possible.
>
> ...
>
> 2.4 When in court,
>
> i. If the employee has to leave the room and leave files unattended, files should be in a locked briefcase or in full view of one or more members of the court party.
> ii. Files can be left unattended in a locked courtroom.
>
> 2.5 At other locations, such as band offices or offices/meeting spaces within courthouses,

i. Files can be left unattended in a locked room for short periods of time (i.e. for a meal).
ii. Files should be left in a locked briefcase if a locked room is not available and only for very short periods of time (i.e. bathroom breaks).

[6] I find that the above policy was not followed in this case. The client file was left unattended on the defence table.

[7] However, even if the above policy was followed, I find the policy itself to be inadequate to protect against the loss of personal information. The policy permits employees to leave personal information unattended for short periods of time in a locked briefcase. The briefcase, even if it is locked, can still be taken with personal information inside of it. My office's position is that these records must be stored securely and kept under the constant control of the employee. If this is not possible, then the records should be temporarily stored in a secure location such as a locked room or desk drawer.

[8] I note that in my office's Investigation Report 226-2017, SLAC indicated that lawyers may be sent to court with multiple briefcases containing paper files. It also said that court may be held in a public location such as a curling rink or a band hall where access to a secure location is unavailable. In those cases, it may not be reasonable nor practical for a lawyer to constantly carry multiple briefcases with him or her.

[9] In a courtroom or in a public place such as a curling rink or band hall, my office recommended to SLAC that it identify threats to the protection of personal information and then identify appropriate safeguards to protect against those threats. Often, this means using multiple layers of safeguards. For example, an unattended locked briefcase in and of itself is not sufficient for protecting personal information in a public location. Fastening the locked briefcase to a fixed object with an anti-theft cable creates an additional barrier to someone who may otherwise walk away with the briefcase. In an email dated January 15, 2018 to my office, SLAC indicated that it is looking into purchasing bike locks so that lawyers can use them to secure briefcases to fixed objects.

[10] Further, in the course of this investigation, my office recommended that SLAC consider converting paper records to electronic records. Then, employees could save the records

electronically to an electronic storage device, which would be much easier to keep under their constant control when they are outside of the office. In response, SLAC indicated that it is ideal that it keep its paper records within its offices and that its lawyers access the material electronically via a password-protected secured device. It said it is improving its own IT infrastructure to enable its lawyers to be able to access records electronically from remote locations. However, that IT infrastructure is not yet in place in all of the locations in which provincial court is held. Therefore, it said that its lawyers will have to continue to carry locked briefcases of material with them to court.

2. Did SLAC respond appropriately to this privacy breach?

[11] A loss of personal information qualifies as a privacy breach. My office recommends that government institutions take the following five steps when responding to a privacy breach:

- Contain the breach,
- Notify affected individuals,
- Investigate the breach,
- Prevent future breaches, and
- Write a privacy breach report.

Contain the breach

[12] To contain a breach is to recover the personal information as much as possible. In this case, that would mean making efforts to recover the missing client file.

[13] SLAC indicated that when the lawyer returned to the courtroom, he had noticed that the client file was missing. In efforts to recover the client file, he talked with others who were in the courtroom, including the following:

- Two defence lawyers who indicated they did not touch, place anything upon, or pick anything from the defence table,
- A third defence lawyer who indicated he had used the defence table but that his folders were black (not blue like the missing client file),
- A fourth defence lawyer who indicated he used the table but did not touch any of lawyer's files,

- The Crown prosecutor, who was using a different table, advised she did not touch any of the lawyer's files but she did indicate she used a copy of the Criminal Code book which was on the defence table,
- A court clerk advised the lawyer that she did not see anyone else approach the defence table.

[14] I find that SLAC has made reasonable efforts to recover the missing client file even though it has not been found.

Notify the affected individual

[15] Notifying the affected individual that her personal information has been lost is important so that she can take necessary steps to protect herself. A notification should include the following elements:

- 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 privacy breaches in the future,
- The 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 Office of the Information and Privacy Commissioner,
- Recognition of the impacts of the breach on affected individuals and an apology.

[16] The lawyer contacted the affected individual by telephone on November 22, 2017, on the same day that the client file was lost. Two days later, he sent an email to the affected individual as a follow up to the telephone call. In the course of this investigation, my office made a recommendation to SLAC to send another notification email containing the following elements:

- describe what personal information was lost,
- explain what types of harm may come to the affected individual as a result of the privacy breach,
- describe steps the affected individual can take to mitigate harm,
- describe the steps that SLAC is undertaking to prevent a similar privacy breach from occurring again,

- explain that the affected individual has a right to complain to my office and provide my office's contact information.

[17] SLAC complied with my office's recommendation and sent a notification dated January 15, 2018 to the affected individual containing the above elements.

[18] I find that SLAC has made reasonable efforts to notify the affected individual of this privacy breach.

Investigate the breach

[19] Investigating privacy breaches to identify factors and/or the root cause is key to understanding what happened and to prevent similar breaches in the future.

[20] As noted earlier, the lawyer did not follow SLAC's *Client Information Management Policy* of keeping the file inside a locked briefcase. Further, my office found that this policy was not adequate to protect against the loss of personal information. I find that these are two factors contributing to this privacy breach.

Preventing future breaches

[21] Preventing future breaches means to implement measures to prevent similar breaches from occurring in the future.

[22] SLAC indicated to my office that it has reminded staff lawyers that court clerks are not responsible for securing client files. It has also reminded its lawyers that if they are sharing a table with other lawyers, there is a risk of co-mingling of files. I find that SLAC's reminders brings awareness to staff lawyers about the risks of losing client files in the courtroom, which is a good first step in preventing future breaches. I find that these reminders, are not sufficient in and of themselves to prevent or minimize the likelihood of a similar privacy breach.

[23] My office had recommended that SLAC amend its *Client Information Management Policy* to indicate that employees must make reasonable efforts to keep records under their constant control when they are outside of the office. If it is not possible to keep records under their constant control, they must keep records in a locked room or locked desk drawer. If a locked room or a locked drawer is not available, then records should be kept in a locked briefcase that is fastened to a fixed object with an anti-theft cable. In an email dated January 15, 2018, SLAC informed my office that it has updated its *Client Information Management Policy* and that its management team is reviewing the updated policy.

Write a privacy breach report

[24] Documenting the privacy breach and the investigation in the matter is a method to ensure that an organization follows through with plans to prevent similar privacy breaches in the future.

[25] SLAC documented its investigation into the privacy breach in a report that it submitted to my office. I find that SLAC has fulfilled this step of responding to a privacy breach.

III FINDINGS

[26] I find that the employee did not follow SLAC's *Client Information Management Policy* in this case.

[27] I find that the version of the *Client Information Management Policy* at the time of the privacy breach to be inadequate to protect against the loss of personal information.

[28] I find that SLAC has made reasonable efforts to recover the missing client file even though it has not been found.

[29] I find that SLAC has made reasonable effort to notify the affected individual of this privacy breach.

[30] I find that SLAC's reminders to its lawyers about court clerks not being responsible for securing client files and there is a risk of co-mingling client files when lawyers share a table in a courtroom are good first steps in preventing future breaches but these reminders are not sufficient in and of themselves to prevent or minimize the likelihood of a similar privacy breach.

[31] I find that SLAC has fulfilled the last step of responding to a privacy breach, which is to write a privacy breach report.

IV RECOMMENDATIONS

[32] I recommend that SLAC make it a regular practice to identify threats to the protection of personal information and then identify appropriate safeguards to protect against those threats, as described at paragraph [9].

[33] I recommend that SLAC follow through with purchasing bike locks, or anti-theft cables, so that its lawyers can use them to secure locked briefcases to fixed objects, as described at paragraph [9].

[34] I recommend that once the updated *Client Information Management Policy* is approved by its management team, as described at paragraph [23], that SLAC provide training to its employees on the new updated policy and provide a copy to my office.

Dated at Regina, in the Province of Saskatchewan, this 18th day of January, 2018.

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