Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 108-2018

Regina Public Library

December 30, 2019

Summary: A Regina Public Library (RPL) employee provided copies of customer incident reports and banning letters, which contained personal information, to a journalist. The journalist later used some of the information, albeit in a non-identifying manner, in a news article. The Commissioner found that a breach occurred, and that the RPL did not have appropriate administrative and technical safeguards in place to help prevent it. The Commissioner recommended that: the RPL update its privacy policies and procedures as well as its service agreements; it provide staff annual privacy training; and it physically limit banning letters to only staff and security guards that require the information to perform their duties.

I BACKGROUND

[1] The Commissioner was formerly a member of the Regina Public Library's (RPL) Board. Although no conflict exists today, the Commissioner has taken no part in this investigation and has delegated the Director of Compliance to make all decisions related to this investigation. The only thing that has occurred is that the Final Report will go out under the Commissioner's name after being reviewed and approved by the Director of Compliance.

[2] On June 13, 2018, the RPL proactively reported a breach to my office. The breach concerned an unknown employee of the central location of the RPL who provided client personal information to a journalist in support of a media story regarding safety and

security at RPL. The information was provided in the form of copies of customer incident reports (IR) and banning letters that were accessed from RPL's intranet by an unknown employee.

[3] The media story, published on May 31, 2018, described incidents the library was having with disruptive and/or abusive customers, which was leaving employees feeling unsafe. Some incidents lead to involvement by the police.

[4] The article further stated that one of the ways that the RPL deals with customers who exhibit extreme behaviour is to ban them for a period of time. This is done by issuing the customer a banning letter.

[5] On June 13, 2018, my office requested that RPL conduct an investigation into the incident and provide its internal investigation report. After receiving the report, it was determined that my office was not satisfied with how the breach was managed, and thus, would be issuing a report.

II DISCUSSION OF THE ISSUES

1. Does *The Local Freedom of Information and Protection of Privacy Act* (LA FOIP) apply?

[6] LA FOIP applies to privacy matters when the following three elements are present: 1) a local authority is involved; 2) there is personal information; and 3) the personal information is in possession or control of the local authority.

[7] The RPL qualifies as a local authority pursuant to subsection 2(f)(vi) of LA FOIP, which provides:

> **2** In this Act:
> …
> (f) "local authority" means:

> …
>
> (vi) the board of a public library within the meaning of *The Public Libraries Act,1984*;

[8] The RPL, therefore, is a local authority pursuant to LA FOIP.

[9] The next step is to determine if personal information is involved. With respect to personal information, subsection 23(1) of LA FOIP provides:

> **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:
>
> …
>
> (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

[10] The RPL did not keep copies of the information that was shared with the journalist, but indicated what was shared was copies of IRs and banning letters. My office contacted the journalist, who confirmed on October 16, 2019, that the documents they received contained the names of the individuals, the library location and a description of the incidents as well as the ban that followed. The journalist confirmed that no addresses were included, and that in one case, a security camera photo was included but that "it was quite grainy". Because names were included with elements such as the reason(s) for which the individuals were banned (which may or may not include the opinions or views on the individual by staff members completing the IRs) as well as in one case, a photo of the individual, I find that personal information was involved.

[11] Finally, the personal information in question was in possession or under the control of the RPL. I find that LA FOIP applies and my office has jurisdiction and authority pursuant to subsection 32(d) of LA FOIP to investigate this matter.

2. Did RPL have authority to disclose the personal information under LA FOIP?

[12] The term "disclosure" means the sharing of personal information with a separate entity that is not a division or branch of the local authority.

[13] The journalist with whom the personal information was shared was not a division or branch of the local authority; this action qualifies as a disclosure under LA FOIP.

[14] Local authorities must disclose personal information in accordance with section 28 of LA FOIP and *The Local Authority Freedom of Information and Protection of Privacy Regulations* (LA FOIP Regulations). Subsection 28(1) of LA FOIP provides:

> **28**(1) No local authority shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individuals to whom the information relates except in accordance with this section or section 29.

[15] A privacy breach occurs when a local authority collects, uses, and/or discloses personal information when not authorized by LA FOIP.

[16] It is clear that the RPL did not have consent pursuant to subsection 28(1) of LA FOIP. It would then have to establish what authority under subsection 28(2) or section 10 of the LA FOIP Regulation that it relied for the disclosure. The RPL did not, in its submission, note if any of these sections would have authorized the disclosure. Based on RPL's submission and my assessment, none of these provisions appear to apply. Thus, I find that a privacy breach occurred.

3. Has the RPL responded to the privacy breach appropriately?

[17] After determining a privacy breach has occurred, the focus of my office becomes one of determining whether or not the local authority appropriately managed the breach. My office needs to be confident that the RPL took the privacy breach seriously and

appropriately addressed it. At the same time, my office needs to be confident that the RPL has taken appropriate steps to prevent similar breaches from occurring in the future.

[18] When a privacy breach occurs, my office suggests that the following five best practice steps be taken by a local authority:

1. Contain the breach;
2. Notify affected individuals;
3. Investigate the breach;
4. Plan for prevention; and
5. Write an investigation report.

[19] Following is an analysis of these steps.

Contain the Breach

[20] Upon learning that a privacy breach has occurred, a local authority 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 has been breached, revoking access privileges, or correcting weaknesses in physical security.

[21] In this case, the RPL did ask the journalist to return the records, who did eventually return them. Although the RPL contained the breach, I do have areas of concern with respect to containment.

[22] RPL advised that it wrote to the journalist approximately one month after learning of the breach and asked them to return the documents. It also asked them to provide written assurance that they did not make or distribute copies, that they would not share names of the customers noted on the documents and that they provide the name(s) of the individual(s) that provided them the documents. According to RPL's submission, it appears it then took the journalist approximately two weeks to courier the records back to the RPL.

[23] Upon learning of a privacy breach, the records should be retrieved immediately. A public body should, whenever possible, make its own attempts to physically retrieve breached documents, such as by going down to the location where the breached documents are located, or sending a courier to pick them up. This minimizes opportunities for further breaches of the information to occur.

[24] I find that the RPL contained the breach, but it should have done so sooner.

Notify the Affected Individual

[25] With respect to notification, LA FOIP provides:

> **28.1** A local authority shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[26] Notifying an individual that their personal information was involved in a privacy breach is important. This is so the affected individual can take measures to protect themselves from potential harm resulting from the breach. It also acknowledges that individuals may feel hurt or humiliated by the type of personal information about them that was breached.

[27] A notification also provides a public body the opportunity to apologize for the breach that has occurred, to reassure individuals that steps have been taken to prevent similar breaches from occurring in the future, and to make individuals aware of their right to raise concerns with my office.

[28] RPL did not know the names of the affected individuals until after the copies of the IRs and banning letters were returned to them. However, it stated that it destroyed the client information as soon as the journalist returned it and, therefore, could not identify who the affected individuals were. RPL indicated it chose not to notify the affected individuals at the time, because it did not feel the breach posed "some risk of damage, detriment or injury to the individual that is significant in nature, that any such damage would only occur in the event of further disclosure by the reporter and since the journalist indicated that [they]

would not disclose the names of the individuals even to us, [they were] aware that the information [they] had constituted a breach of privacy".

[29] My office's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities*, states that providing notification to an affected individual must pose "some risk of damage, detriment or injury to the individual that is significant in nature", such as bodily harm, humiliation or damage to reputation. There must be harm that comes to the individual whose information was breached as a result of notification provided by the local authority to the affected individual. In this case, the RPL did not elaborate as to how it arrived at its conclusion that if it provided notification to the affected individuals, that the notification would pose a risk of harm to them.

[30] I find that RPL did not provide notification and that it should have in place policies and guidelines to assist in assessing the risk of harm with respect to notifying affected individuals. When my office is undertaking an investigation, local authorities should not destroy information that I may require to complete my investigation, including copies of the personal information that has been breached.

Investigate the Breach

[31] Once a breach is contained and appropriate notification has occurred, the public body should conduct an internal investigation so that it can understand what led to the privacy breach. This can be accomplished by undertaking a root cause analysis. The investigation should also consider whether there were adequate safeguards in place at the time of the breach. This analysis helps with implementing a plan to prevent similar breaches from occurring again in the future.

[32] Pursuant to section 23.1 of LA FOIP, local authorities have the duty to protect information that is in its possession or control including having established, "polices and procedures to maintain administrative, technical and physical safeguards…" Safeguards are the measures or controls a local authority puts in place to help it protect personal information that is in its possession or control.

[33] RPL provided my office with a copy of its confidentiality policy. While it has a policy, the question becomes whether or not RPL's policy is adequate to support its obligations under LA FOIP. Upon review of RPL's confidentiality policy, I note several deficiencies that I recommend RPL address:

- The policy does not mention LA FOIP as its legislative authority respecting the collection, use and disclosure of personal information. It is ideal that any organization that is subject to LA FOIP acknowledge this authority so that employees and others are aware of the authority and their obligations under this legislation.

- The policy does not fully establish RPL's purpose for collecting personal information (e.g. to issue library cards, manage lending). Instead, the policy appears to leave the use or disclosure of personal information up to each employee's discretion, which is not definitive and may not always comply with the law.

- RPL applies the policy to staff and volunteers, but does not indicate whether or not it applies to security guards who act under RPL's services agreement with a private security company.

- A review of the security services agreement, which RPL provided my office, also excludes a reference to LA FOIP, and does not establish the purpose for which security guards may or may not collect, use and disclose personal information. Pursuant to subsection 2(b.1) of LA FOIP, individuals retained under contract have the same obligations under LA FOIP as employees do. Neither RPL's policy nor services agreement acknowledges this.

- While RPL does require staff and security personnel to sign a stand-alone confidentiality oath when they commence employment - a copy of which they provided to my office - I note that the oath copies wording from RPL's confidentiality policy, which I already concluded is deficient. While the oath does state the consequences for not complying with the oath, the oath itself does not properly identify under what authority employees or security guards may or may not use and disclose personal information.

[34] Similar to its policies, the RPL's service agreements should include what duties and obligations contractors (in this case, security guards) have with respect to LA FOIP. My office's *Best Practices for Information Sharing Agreements*, provides guidance on developing information sharing agreements where personal information is involved.

[35] To support employees and volunteers in understanding their obligations, including following established policies and procedures, local authorities should make available annual privacy training. The British Columbia Information and Privacy Commissioner stated in its Investigation Report P19-01 at paragraph [4.12] that not having proper privacy training, "increases the risk of a significant privacy breach, especially as personal information is increasingly collected, used, disclosed and stored in digital formats."

[36] Staff, contractors and volunteers should also be adequately trained, so that they understand their obligations under privacy legislation and internal privacy policies and procedures. The RPL stated that it does not require employees or contractors to take any privacy training. If a local authority does not have privacy training material, it does not have start from scratch as many online resources exist. For example, as a starting point, the RPL may refer to the Ministry of Justice's freely available online training created specifically for local authorities. I recommend that RPL equip its staff and others by providing annual privacy training.

[37] Policies and procedures should be complemented by physical and technical safeguards. In my Investigation Report 260-2017, my office discussed some technical safeguards that can help a public body prevent breaches, including authentication, secure log-on procedures and system auditing. These are all safeguards that complement and support policies, procedures and training. Other considerations may include placing 'read only' functions on documents that do not allow printing or attaching sensitive information to emails, having role-based access (i.e. limiting who can access what), having staff routinely lock their work stations or change/update their passwords, undertaking proactive auditing and monitoring, and ensuring accounts are deactivated immediately when staff are no longer actively employed.

[38] Another technical safeguard is proactive system auditing. In my Review Report 260-2017 at paragraph [33], my office commented as follows:

> Auditing is a technical safeguard and is necessary to assess compliance with and measure effectiveness of policies and procedures, assess compliance with legislation, assess if appropriate measures are in place to control access and monitor access.

[39] The RPL stated to my office that as part of its investigation of the breach, it did not conduct extensive auditing of printer logs and staff email to narrow down which staff committed the breach. It noted it would have had difficulty doing so because of: the volume of records involved; multiple front-desk staff using one intranet account; and concern over violating the privacy of staff by accessing their mailboxes.

[40] In Investigation Report 090-2017, my office reviewed the matter of a City of Saskatoon bus driver who alleged their privacy was breached when the City used video surveillance footage installed on a city bus to investigate a complaint against them. My office determined, in this matter, that the City had authority under LA FOIP to collect and use the employee's information in the manner in which it did because it did so in such a way that it was limited to aid the investigation.

[41] Thus, the RPL would have been able to search the emails of employees to determine whether the breached information originated from their email. Attempts to investigate this way should be reasonable, and should follow some established procedure or protocol that limits the search to the purpose or need. In this case, for example, a search could have been limited to identifying the approximate date range of when the breach occurred, those staff on duty during that time, and from which terminal the breach likely originated after other interventions had failed (e.g. interviewing employees).

[42] I do note that likely one of the greatest factors that would hinder the RPL from narrowing down which staff committed the breach is having multiple system users access the intranet and other systems through one account. When a breach occurs, a local authority would not have the ability to appropriately review staff activity if staff do not have their own log-on credentials. RPL should have accounts for each staff member, and each staff member should have their own logon credentials.

[43] I find that the RPL did not conduct a thorough investigation into this incident, and that the root cause was that the RPL did not have appropriate administrative and technical safeguards in place that could have helped to prevent it.

[44] I wish to add that during my review of this breach, the RPL stated that banning letters, which contain personal information, are available to all staff on the intranet, whether they work with the public or not. This may lead to further disclosures and privacy breaches. One of the principles that underlies Part IV of LA FOIP is the "need-to-know" principle, wherein only those with a legitimate need to know personal information in order to carry out their duties should have access to it. I discussed this principle in my recent Investigation Report 074-2018, 075-2018. As part of its technical controls, I recommend that the RPL consider how it can physically limit the banning letters to only staff and security guards with a need-to-know (i.e. to enforce the ban), or consider some other way of providing this information to staff and security guards who require it.

Plan for Prevention

[45] Prevention is perhaps the most important step in responding to a privacy breach. While a privacy breach cannot be undone, an organization can learn from and improve its practices. To avoid future breaches, an organization 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.

[46] In its submission, the RPL noted it had updated guidelines and procedures for completing and maintaining IRs and banning letters. It noted staff undertook training to make information less vulnerable, but do not note what that training was or if it is intended to be ongoing (although it has indicated to my office that it did not offer or make available regular privacy training). Another step it took was to review with all staff, jointly with the union, RPL's confidentiality policy and asked staff to sign the policy acknowledging their agreement with it. However, as noted previously in this Report, the existing policy is deficient.

[47] As I have laid out in this Report, there are many further steps the RPL can take to prevent similar breaches from occurring in the future. As such, I find that the RPL does not have an adequate plan for prevention.

Write an Investigation Report

[48] The final step in managing a privacy breach is to prepare the report. Documenting an organization's investigation into a privacy breach is a method to ensure that the organization follows through with plans to prevent similar breaches in the future.

[49] RPL provided my office with its internal investigation report and complied with all follow-up requests for information and clarification. I find that the RPL has fulfilled this step in responding to a privacy breach.

III FINDINGS

[50] I find that LA FOIP is engaged.

[51] I find that a privacy breach occurred.

[52] I find that the RPL contained the breach, but it should have done so sooner.

[53] I find that the RPL did not provide notification.

[54] I find that the RPL did not conduct a thorough investigation into this incident, and that the root cause was that the RPL did not have appropriate administrative and technical safeguards in place that could have helped to prevent it.

[55] I find that the RPL does not have an adequate plan for prevention.

IV RECOMMENDATIONS

[56] I recommend that the RPL update its policies and procedures to include RPL's privacy obligations under LA FOIP with respect to the protection, collection, use and disclosure of personal information. These policies and procedures should further establish to which personnel (e.g. staff, contracted individuals, volunteers) these polices and procedures apply.

[57] I recommend that RPL equip its staff and others by providing annual privacy training.

[58] I recommend that, similar to its policies, the RPL's service agreements should include what duties and obligations contractors (in this case, security guards) have with respect to LA FOIP.

[59] I recommend that the RPL consider how it can physically limit the banning letters to only staff and security guards with a need-to-know (i.e. to enforce the ban), or consider some other way of providing this information to staff and security guards who require it.

Dated at Regina, in the Province of Saskatchewan, this 30th day of December, 2019.

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