Office of the Information and
Privacy Commissioner of Alberta

Investigation Report F2018-IR-03

Investigation into an unauthorized disclosure of personal information by the City of Calgary

September 21, 2018

City of Calgary

Investigation 003800

Summary

On June 28, 2016, the City of Calgary voluntarily reported a privacy breach to the Office of the Information and Privacy Commissioner (OIPC) under the *Freedom of Information and Protection of Privacy Act* (FOIP Act). The City of Calgary also notified individuals affected by the breach on or around August 15, 2016.

Upon being notified, seven affected individuals submitted privacy complaints to the OIPC. Rather than investigate each complaint individually, the Commissioner opened an investigation on her own motion to address the concerns raised by the complainants.

The City of Calgary reported that the breach occurred when an employee, who was "seeking technical assistance from a close contact" on two different job assignments, disclosed spreadsheets containing personal information without authorization. The recipient was an employee with another municipality. The spreadsheets were emailed to the recipient's work and personal email addresses and contained information on occupational health and safety incidents the City of Calgary reported to the Workers' Compensation Board (WCB) between 2012 and 2016, concerning 3,123 City of Calgary employees.

The investigation found, and the City of Calgary acknowledged, that sending the emails and attachments to the "close contact" constituted an unauthorized disclosure in contravention of Part 2 of the FOIP Act.

The investigation also found that the City of Calgary's physical and technical safeguards are typical of what public bodies generally implement. However, a breach response protocol had not been formally established as an administrative safeguard at the time of this incident. The City of Calgary indicated that "…the plan is to develop a process for future breaches".

The investigation recommended that the City of Calgary complete its work to develop and communicate a breach response protocol to all staff.

Considering the concerns raised by some of the affected individuals in their complaints to the OIPC, the investigation also reviewed the City of Calgary's breach response.

The review found the City of Calgary followed the four key steps in responding to a breach, as set out in the OIPC's *Key Steps in Responding to Privacy Breaches* guidance document:

1. The City of Calgary's actions to contain the breach were timely and appropriate in the circumstances. The recipient and the recipient's employer confirmed all documents were deleted and not disclosed further.

2. The City of Calgary made a reasonable assessment of the risks to affected individuals.

3. The City of Calgary made a decision to notify, and directly notified affected individuals through registered mail, as well as indirectly through other means (e.g. news release).

4. Since the incident occurred, and during this investigation, the City of Calgary took preventative steps to reduce the risk of a reoccurrence.

Table of Contents

Background 7
Jurisdiction 7
Issues 9
Methodology 9
Analysis and Findings 9
Issue 1: Did the Public Body disclose personal information in compliance with Part 2 of the FOIP Act? 9
Issue 2: Did the Public Body protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction as required under section 38 of the FOIP Act? 11
Breach Response 14
Step One: Contain the Breach 14
Step Two: Evaluate the Risks Associated with the Breach 15
Step Three: Breach Notification and Reporting 16
Step Four: Prevention 17
Summary of Findings and Recommendation 18

Background

[1] On June 28, 2016, the Office of the Information and Privacy Commissioner (OIPC) received a report from the City of Calgary (the Public Body) about a possible breach of the *Freedom of Information and Protection of Privacy Act* (FOIP Act). The Public Body reported that an employee (the Employee) disclosed information about workplace injury claims to an employee of another municipality (the Recipient). On July 19, 2016, the OIPC opened a file to review the City of Calgary's breach report.

[2] On or around August 15, 2016, as part of its response to the breach, the Public Body wrote to affected individuals to advise them about the "Information Disclosure". Among other things, the letter said, "The City has informed and is working with the [OIPC] on this matter." The Public Body provided contact information should any affected individuals "wish to register a formal complaint with the OIPC".

[3] After receiving the Public Body's letter, a number of individuals submitted written complaints to the OIPC. These individuals generally said they were complaining that their personal information had been disclosed in contravention of Alberta's privacy laws. In addition, some complainants expressed concerns regarding the Public Body's handling of the breach (e.g. "if 'low risk' why all the fuss" and "the City was not overly forthcoming with the exact information shared and where it was sent").

[4] In total, the OIPC received seven written complaints from affected individuals. Rather than investigate each complaint individually, the Commissioner decided to open a single investigation on her own motion, pursuant to section 53(1)(a) of the FOIP Act, to address the concerns raised by the complainants. The investigation was opened on September 21, 2016.

[5] The Public Body was advised that the issues for the investigation were as follows:

- Did the Public Body disclose personal information in compliance with Part 2 of the FOIP Act?
- Did the Public Body protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction as required under section 38 of the FOIP Act?

[6] The file was initially assigned to another investigator and was subsequently transferred to me. This report sets out my findings and recommendations.

Jurisdiction

[7] The FOIP Act applies to all records in the custody or under the control of a public body. The definition of "public body" includes "a local public body" (section 1(p)(vii)). A local public body includes "a local government body" (section 1(j)(iii)). A local government body includes "a municipality as defined in the *Municipal Government Act"* (section 1(i)(i)).

[8] The City of Calgary is a municipality as defined in the *Municipal Government Act* and is therefore a public body subject to the provisions of the FOIP Act.

[9] Section 1(n) of the FOIP Act defines "personal information" as follows:

> (n) "personal information" means recorded information about an identifiable individual, including
>
> (i) the individual's name, home or business address or home or business telephone number
>
> …
>
> (iv) an identifying number, symbol or other particular assigned to the individual, …
>
> (vi) information about the individual's health and health care history, including information about a physical or mental disability,
>
> (vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given

[10] The breach involves emails sent by the Employee of the Public Body to an employee of another municipality. Documents attached to these emails included information related to occupational health and safety incidents the Public Body reported to the Workers' Compensation Board (WCB) between 2012 and 2016, concerning 3,123 employees of the Public Body.

[11] The Public Body provided me with copies of the emails and spreadsheet attachments, which contained the following information:

- name of employee,
- employee ID,
- Public Body's WCB account number,
- business unit and division,
- description of the employee's occupation,
- WCB claim numbers,
- date of incident,
- brief description of the incident,
- nature of the injury,
- body part injured,
- type (medical, aid or time loss claim),
- status of WCB claim (accepted or denied by WCB),
- costs associated with the claim,
- days lost from work, and
- modified work offered.

[12] This information is recorded information about identifiable individuals, and reveals part of their employment history with the Public Body, as well as details about their health care history. The information qualifies as "personal information" under section 1(n) of the FOIP Act.

Issues

[13] The following issues were identified for this investigation:

- Did the Public Body disclose personal information in compliance with Part 2 of the FOIP Act?
- Did the Public Body protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction as required under section 38 of the FOIP Act?

[14] Because some of the individuals who submitted complaints to the OIPC raised concerns about the Public Body's handling of the breach, I also reviewed the Public Body's breach response.

Methodology

[15] As part of my investigation, I reviewed documentation provided to me by the Public Body, including the original report of the breach to the OIPC and follow-up correspondence, the emails and attachments at issue, the Public Body's responses to questions I asked, information about the role and responsibilities and relevant employment information of the Employee who sent the emails, as well as the Public Body's policies and procedures.

Analysis and Findings

Issue 1: Did the Public Body disclose personal information in compliance with Part 2 of the FOIP Act?

[16] Part 2 of the FOIP Act deals with protection of privacy, including use and disclosure of personal information by public bodies. Section 40 of the FOIP Act is found in Part 2, and sets out the circumstances in which a public body is authorized to disclose personal information.

[17] In this case, the Employee used his work-provided email account to send emails with attached personal information to an unauthorized recipient at another municipality.

[18] With respect to the Employee's access to and use of the personal information at issue, the Public Body reported that:

> [The Public Body employee] had legitimate business need to access this material. Staff in this role are required to access and audit the WCB records of all claims for all employees in the Corporation to ensure accuracy and timelines of provided reporting to WCB.

[19] Further:

> The use of this material was for two unique but similar assignments:
>
> **Assignment 1- June 14, 2016:** Employee was asked to compare the excel spreadsheet with the pdf files using the WCB claim number. The employee was to confirm column Q on the spreadsheet using the pdf files as the data authority. All changes were to be highlighted in yellow.
>
> **Assignment 2 – June 15, 2016:** The employee was asked to verify which of the files on the spreadsheets were files where the other party was at fault. The task required the employee to compare the spreadsheet data against a corporate internal database. The employee chose to add a column to the spreadsheet to complete that verification.

[20] In completing these assignments, the Employee sent emails to the Recipient's work and personal email address (June 14, 2016), and then to the Recipient's work email address (June 15, 2016), disclosing the personal information at issue in attachments to the emails.

[21] I reviewed copies of the email exchanges between the Employee and the Recipient as well as the attached documents. The emails and attachments are clearly intended to request assistance in completing the two assignments described above; specifically, the Employee asked how to compare the various sources of information and update the spreadsheets accordingly.

[22] I asked the Public Body if it was correct that the Public Body "…considered the disclosure of the information at issue an unauthorized disclosure of personal information, meaning that it was not allowed under section 40 of the FOIP Act[?]". The Public Body confirmed that sending the emails and attachments constituted an unauthorized disclosure.

Finding

[23] The copies of the emails and attachments provided to me by the Public Body support the finding that the email correspondence between the Employee and the Recipient contained personal information, and was an unauthorized disclosure of personal information, in contravention of section 40 of the FOIP Act.

[24] Since the Employee was working for the Public Body at the time he sent the emails, I find that the Public Body disclosed personal information in contravention of Part 2 of the FOIP Act.

Issue 2: Did the Public Body protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction as required under section 38 of the FOIP Act?

[25] Public bodies subject to the FOIP Act have a duty to protect personal information. Section 38 of the FOIP Act reads:

> The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

[26] Section 38 requires public bodies to make reasonable security arrangements to protect personal information against a number of risks, including unauthorized access and disclosure. Safeguards must be reasonable; they do not need to be perfect. Unauthorized use and disclosure of personal information may still occur even when reasonable security arrangements have been implemented.

[27] The OIPC has consistently urged all entities subject to Alberta's privacy laws to implement three layers of safeguards: physical, administrative and technical (see OIPC Investigation Reports P2006-IR-005, H2006-IR-002, H2007-IR-002 and F2013-IR-01, for example).[1]

[28] In order to assess the Public Body's compliance with the requirements under section 38 of the FOIP Act, I asked the Public Body to provide me with evidence concerning its administrative, technical and physical security arrangements relevant to this incident.

Administrative Safeguards

[29] Administrative safeguards typically include policies and procedures, confidentiality oaths, and training. In this case, the Public Body reported that it "…has implemented policies and procedures that guide the protection and handling of information and the secure use of technology". The Public Body provided me with copies of relevant policies and procedures, including the "Acceptable Use of City Technology Resources" and "Information Security Classification and Control" policies and procedures.[2]

[30] Notably, the Public Body did not provide a copy of a breach response protocol. Instead, the Public Body reported that, as a result of this incident and in order to ensure a robust response, "…the plan is to develop a process for future breaches".

[31] The Public Body also described its "On-boarding Process for new or transferred employee[s]" and provided me with copies of forms completed by the Employee at the time of hire.

[32] The Public Body's "General Confidentiality and Privacy Acknowledgement" form addresses confidentiality requirements for employees of the Public Body, and sets the expectation that

[1] OIPC investigation reports are available at https://www.oipc.ab.ca/decisions/investigation-reports.aspx.
[2] The Public Body has also made these policies and procedures publicly available at https://www.calgary.ca/CA/cmo/Pages/General-Administration-Policies.aspx.

employees will hold information in the workplace in confidence, and only use it as required by their work duties. The form reads, in part, as follows:

> I (name) ….understand that as an employee of The City of Calgary, I am expected to abide by all legislation and policies regarding confidentiality and protection of personal information and proprietary information under the custody and control of The City of Calgary. This includes but is not limited to:
>
> - The Alberta Freedom of Information and Protection of Privacy Act (FOIP)
>
> …
>
> With respect to all personal and proprietary information in any format, I understand that the above policies and FOIP legislation require me:
>
> 1. To maintain all such information in strict confidence at all times and in all places and not to publish, sell, distribute or otherwise disclose this information except to the FOIP Program Administrator or with the prior consent of a Business Unit Manager.

[33] The Employee signed this form on June 10, 2016. A tick box indicating "I have received information on FOIP and reviewed the relevant policies" is checked affirmatively.

[34] The Public Body also provided me with a copy of its "Supervisor Checklist for New Employee" form, which was also signed by the Employee and his supervisor on June 10, 2016. This checklist indicates that the Employee took the "City of Calgary Orientation" training (COCO). The Public Body reported that:

> COCO includes the Municipal Handbook which states that FOIP has been in effect at The City of Calgary since 1999 and that The City dedicates itself to (...) ensuring the protection of individual privacy. It provides a link for information about FOIP. COCO also requires that the employee review the Code of Conduct, Corporate Security's intranet site which has multiple resources on information security, and the Information Security intranet site which provides multiple resources on privacy protection.

[35] In addition, the Public Body indicated that:

> At that time [the Employee signed off on the checklist], the supervisor verbally set expectations regarding privacy and confidentiality of information that [the Employee] had access to and would handle in the course of his duties.

Physical and Technical Safeguards

[36] The Public Body provided me with a written description of its physical and technical safeguards relevant to this matter.

[37] The physical safeguards in place included limited access to computer workstations, passcard locks, computer screen locks and monitoring by supervisors.

[38] Technical safeguards included network security tools (e.g. firewalls, URL filtering), limiting access to information on a need-to-know basis, network segregation, automatic computer

screen locks, as well as monitoring and auditing networks and information accessed on a set schedule.

Findings

[39] In my view, the Public Body's physical and technical safeguards are typical of what public bodies generally implement, and are appropriate for the information technology and information assets used by the Employee in his job role.

[40] Documentation provided to me demonstrates that the Employee undertook the onboarding activities required of all new Public Body employees and received training related to privacy and confidentiality, as per the Public Body's processes. These processes are reasonable administrative safeguards. However, I found the Public Body had not established a breach response protocol as an administrative safeguard at the time of this incident.

[41] Previous investigation reports by the OIPC under the *Health Information Act* have established that implementing a breach response protocol is an essential component of meeting legislated requirements to safeguard health information.[3,4] Additionally, when the OIPC reviews privacy impact assessments (PIAs) of custodians' administrative policies, the OIPC ensures breach response policies and protocols are in place prior to the acceptance of PIAs. The OIPC has also recommended that custodians provide regular reminders to staff about breach policies and procedures for successful breach management. The same would hold true for public bodies under the FOIP Act.

Recommendation

- I recommend that the Public Body complete its work to develop and communicate a breach response protocol to all staff.

[3] See *Investigation Report H2014-IR-01: Report concerning theft of unencrypted laptop containing health information*, available at https://www.oipc.ab.ca/media/531208/h2014-001ir.pdf.
[4] See *Investigation Report H2015-IR-01: Privacy breach reporting in Alberta's health sector*, available at https://www.oipc.ab.ca/media/621630/H2015-IR-01.pdf.

Breach Response

[42] As part of my investigation of this matter, and considering the concerns raised by some of the complainants in their submissions to the OIPC, I reviewed the Public Body's response to the breach.

[43] Under the FOIP Act, public bodies have no legal requirement or duty to notify the Commissioner of a privacy breach, and no legal requirement to notify individuals affected by a breach. Further, the Commissioner does not have the power to require that public bodies notify individuals about privacy breaches, or set terms and conditions regarding the timeliness and form of notification. Duties to notify are not FOIP Act compliance issues.

[44] Nonetheless, a public body should have a breach response protocol implemented as a reasonable administrative safeguard under the FOIP Act.

[45] The OIPC has published a number of guidance documents on its website to assist organizations, custodians and public bodies in responding to privacy breaches. In particular, *Key Steps in Responding to a Privacy Breach* (the Guide) was originally published in 2006, and subsequently revised and updated, most recently in August 2018.[5] The Guide sets out four key steps in responding to a privacy breach. The best practices in the Guide, including the four key steps, are very similar to those included in breach response guidelines issued by the Office of the Information and Privacy Commissioner for British Columbia, the Information and Privacy Commissioner of Ontario and the Office of the Privacy Commissioner of Canada.

[46] I have reviewed the Public Body's response to this breach against the four key steps for responding to a privacy breach, as outlined in the Guide.

Step One: Contain the Breach

[47] The Guide recommends that, in the event of a privacy breach, a public body should take immediate steps to limit the breach by containing it (e.g. stop the unauthorized practice, recover the records, shut down the system, revoke access), ensure the staff responsible for privacy are made aware, and notify the police if theft or other criminal activity are at issue.

[48] Actions that could be taken to contain a breach resulting from unauthorized disclosure of information via email include discontinuing access to information systems, contacting the recipient(s) of the information, and obtaining an undertaking confirming that the personal information has not been viewed, used, or disclosed further, and has been securely destroyed.

[5] *Key Steps in Responding to Privacy Breaches* is available at https://www.oipc.ab.ca/media/950540/guide_key_steps_breach_response_aug2018.pdf.

[49] In this case, the Public Body reported that it undertook the following steps to contain the breach:

- suspended the Employee on June 21, 2016, the day the Public Body uncovered the emails from the Employee to the Recipient;
- suspended all of the Employee's accounts on the Public Body's information systems;
- obtained assurances from both the Employee and Recipient that the information was not further disclosed and that all copies of the emails and attachments in question were deleted; and
- contacted the Recipient's employer (another municipality subject to the FOIP Act) on June 23, 2016, and obtained confirmation that the personal information in question had been deleted from the employer's information systems.

[50] I consider that the Public Body's actions to contain the incident were timely and appropriate in the circumstances.

Step Two: Evaluate the Risks Associated with the Breach

[51] The second step in responding to a privacy breach is to evaluate the associated risks. A number of factors to be considered are set out in the Guide, including the nature of the information involved, the cause and extent of the breach, the individuals affected by the breach, and the possible harm that could result from the breach.

[52] The Public Body formally reported this matter to the OIPC on June 28, 2016. At the time, the Public Body assessed the type of harm that might result from the breach as follows:

> Harm from this release could compromise a person's ability to obtain medical services, harm or damage personal reputation, reveals information about their health that could affect eligibility for insurance coverage or affect ability to obtain employment.

[53] The Public Body also noted that "level of sensitivity is high as it contains medical information".

[54] In assessing the likelihood that harm could result from the incident, the Public Body initially reported:

> We are not sure who has been given access to the information beyond the staff member at [the other municipality]. We have received an explanation from our staff member that they did not know how to add a column and contacted a known person at [the other municipality], they also sent the first email to that known person's gmail account. It is impossible for us to know who else has the information.

[55] Subsequently, after the Public Body had further investigated the incident, it assessed that there was a "very low risk" of harm, advising affected individuals that…

> …the disclosure occurred when a City employee was seeking technical assistance from a close contact. We do not believe that the information was disclosed maliciously or for personal gain. There was only one recipient. The recipient works at another Alberta municipality and received this information at their personal and work email addresses. We contacted both the recipient

> and the recipient's employer and we have been advised that the information was not shared further and was deleted.

[56] In considering the fact that the personal information at issue includes highly sensitive identifying information (i.e. medical information) that could be used to cause the harms of hurt and/or humiliation to the affected individuals, I agree with the Public Body's assessment of the types of harm that could result from this breach.

[57] I also agree with the Public Body that the likelihood of harm resulting from the breach is low, given the circumstances. There is no evidence of malicious intent or purpose; rather, the Employee was clearly seeking assistance in completing a work assignment. Although the information was exposed for seven days it was provided to one recipient who is a known and close contact of the Employee who sent the emails. There is no reason to believe that the Recipient would have any motive or cause to use or disclose the personal information further. The Public Body very quickly contacted the Recipient and his employer (another municipality, also subject to the FOIP Act) and received assurances that the information in question was not disclosed further, and was deleted from the employer's information systems.

Step Three: Breach Notification and Reporting

[58] The third step set out in the Guide is to consider whether notification of the affected individuals is necessary in order to avoid or mitigate harm. As previously noted, the Commissioner does not have the power to require that public bodies notify individuals about privacy breaches, or set terms and conditions regarding the timeliness and form of notification. These matters are not FOIP Act compliance issues; however, the OIPC will provide general advice and guidance to inform a public body's decision-making.

[59] In this case, the Public Body explained that even though it believed the likelihood of harm was low "the City's senior management felt that notifying affected individuals was the right thing to do". The Public Body consulted with, and provided updates to, the OIPC on steps it was taking to respond to the breach, including its plans to notify affected individuals.

[60] On August 11, 2016, the Public Body confirmed to the OIPC that it notified the following groups of individuals via registered letters:

- current employees,
- former employees, and
- executors of former employees' estates, where applicable.

[61] The Public Body also notified the FOIP Office of the Calgary Police Service in relation to those Public Body employees who worked for the Calgary Police Service and who were affected by the breach.

[62] In addition, the Public Body issued a press release about the incident, and dedicated certain staff members to respond to any questions from affected individuals. The Public Body also offered to provide affected individuals with copies of the information about them that was in the email attachments, upon request.

[63] With respect to timing, the Guide states, "The most important step you can take is to respond immediately to the breach." It also says, "Notification of individuals affected by the breach should occur as soon as possible following the breach."

[64] In this case, the Public Body reported that it took more time than expected to validate addresses for certain groups of affected individuals, in particular for the representatives of deceased persons.

[65] Finally, the Guide says consideration should be given to notifying parties other than the affected individuals. In this case, the Public Body notified the relevant union representatives, and sent a formal report of the breach to the OIPC.

Step Four: Prevention

[66] With respect to the four key steps in responding to a privacy breach, the Guide states, "You should undertake steps one, two and three immediately following the breach and do so simultaneously or in quick succession. Step Four provides information for longer-term prevention strategies."

[67] Following the best practices set out in the Guide, the final step in responding to a breach involves a thorough investigation of the cause of the breach, and developing, or improving as necessary, long-term safeguards to protect against further breaches. Policies may need to be reviewed and updated, staff training should be undertaken to ensure employees are aware of their responsibilities. An audit should be conducted at the end of the process to ensure that the prevention plan has been fully implemented. In this case, as part of the information originally provided to the OIPC about the breach, the Public Body reported it was taking the following actions:

- dedicated three employees on the Corporate Security Team to specifically respond to breaches of this nature;
- started a full review of current processes and information security safeguards to prevent a future reoccurrence; and
- initiated the development of a process for future breaches, involving law, security, the FOIP Office and Corporate Issues Management, in order to identify "who needs to be involved, the roles each party has to play and steps to be taken to contain the breach, make a response, investigate and notify those affected by the breach".

Overall Assessment of Breach Response

[68] In my view, the Public Body followed the four key steps in responding to a breach, as set out in the Guide. The Public Body's actions to contain the breach were timely and appropriate in the circumstances. The Public Body assessed the risks to affected individuals, made a decision to notify, and directly notified affected individuals through registered mail, as well as indirectly through other means. Since the incident occurred, and during this investigation, the Public Body has taken preventative steps to reduce the risk of a reoccurrence.

Summary of Findings and Recommendation

[69] My findings from this investigation are as follows:

- The email correspondence between the Employee and the Recipient contained personal information, and was an unauthorized disclosure of personal information, in contravention of section 40 of the FOIP Act.
- Since the Employee was working for the Public Body at the time he sent the emails, I find that the Public Body disclosed personal information in contravention of Part 2 of the FOIP Act.
- The Public Body's physical and technical safeguards are typical of what public bodies generally implement, and are appropriate for the information technology and information assets used by the Employee in his job role.
- Documentation provided to me demonstrates that the Employee undertook the onboarding activities required of all new Public Body employees and received training related to privacy and confidentiality, as per the Public Body's processes. These processes are reasonable administrative safeguards.
- The Public Body had not established a breach response protocol as an administrative safeguard at the time of this incident. Previous investigation reports by the OIPC under the *Health Information Act* have established that implementing a breach response protocol is an essential component of meeting legislated requirements to safeguard health information. Additionally, when the OIPC reviews privacy impact assessments (PIAs) of custodians' administrative policies, the OIPC ensures breach response policies and protocols are in place prior to the acceptance of PIAs. The OIPC has also recommended that custodians provide regular reminders to staff about breach policies and procedures for successful breach management. The same would hold true for public bodies under the FOIP Act.
- The Public Body followed the four key steps in responding to a breach, as set out in the Guide. The Public Body's actions to contain the breach were timely and appropriate in the circumstances. The Public Body assessed the risks to affected individuals, made a decision to notify, and directly notified affected individuals through registered mail, as well as indirectly through other means. Since the incident occurred, and during this investigation, the Public Body has taken preventative steps to reduce the risk of a reoccurrence.

[70] Based on the findings, I recommend that the Public Body complete its work to develop and communicate a breach response protocol to all staff.

[71] I appreciate the Public Body's cooperation throughout this investigation.

Chris Stinner
Manager – Special Projects and Investigations