Alberta Information and Privacy Commissioner

Investigation regarding the collection, use and disclosure of personal information by Alberta Justice and Attorney General

October 21, 2010

(Investigation F5362, F5363, F5364, F5365, F5366, F5367, F5368, F5371, F5372, F5373, F5374, F5375, F5379, F5380, F5383, F5384, F5385, F5386, F5387, F5393, F5394, F5395, F5397, F5398 and F5413)

Investigation Report F2010-IR-001

I. INTRODUCTION

[1] From April 30, 2010 to June 1, 2010, the Information and Privacy Commissioner ("the Commissioner") received twenty-five letters of complaint from employees with Alberta Justice and Attorney General ("the Public Body"). All employees work in the Public Body's Maintenance Enforcement Program ("MEP"). The employees will be referred hereinafter collectively as "the Complainants" or singularly "the Complainant".

[2] Each Complainant alleged that the Public Body violated their privacy by conducting a credit check on them without their knowledge or consent. Most of the Complainants used the following (or similar) wording in their written complaint to our office:

> *"This letter is to inform you of a violation of the Freedom of Information and Protection of Privacy Act (FOIP) by Alberta Justice, Maintenance Enforcement Program (MEP).*
>
> *…On January 18, 2010, Alberta Justice conducted an unauthorized Equifax credit check on myself in order to determine whether or not I had or was in "financial distress". This check was done in conjunction with an ongoing internal investigation regarding fraudulent cheques that were being circulated by an outside party. Alberta Justice did not have my authorization to perform this credit check. Alberta Justice illegally collected my personal and private information in order to perform these checks. I was not notified of this credit check until April 23, 2010 [some complainants wrote "April 27, 2010"].*
>
> *…I am requesting that the commissioner commence a full investigation as to why Alberta Justice violated their employees' privacy and what can be done to correct this breach of trust. I would like to know who authorized these checks. Who provided the individual in question my personal and private information, and what can be done to reverse this infringement of my privacy."*

II. COMMISSIONER'S AUTHORITY

[3] Under section 65(3) of the *Freedom of Information and Protection of Privacy Act* ("the FOIP Act" or "the Act"), a person who believes that their own personal information has been collected, used or disclosed by a public body in contravention of Part 2 of the FOIP Act may ask the Commissioner to review the matter.

[4] Section 65(3) grants each of the Complainants a right to ask for a review. A right to ask for a review under section 65(3) can give rise to an inquiry. So that each Complainant may exercise their rights under section 65(3) of the FOIP Act, the Commissioner opened 25 separate cases.

[5] The FOIP Act authorizes the Commissioner to conduct investigations to ensure compliance with any provisions of the Act (section 53(1)(a)) and to investigate complaints regarding the collection, use and disclosure of personal information (section 53(2)(e)).

[6] The Commissioner authorized me to investigate and try to settle any matter that is the subject of the complaints. As the subject matter of the twenty-five complaints is the same, I have prepared one investigation report in relation to my findings and recommendations.

III. PRELIMINARY MATTERS

Does the *Personal Information Protection Act (PIPA)* apply?

[7] Twenty-one of the Complainants alleged that the Public Body violated both the FOIP Act and the *Personal Information Protection Act* (PIPA). However, section 4(2) of PIPA reads:

> *4(2) Subject to the regulations, this Act does not apply to a public body or any personal information that is in the custody or under the control of a public body.*

[8] The Public Body is a "public body" as defined by section 1(p)(i) of the Act. Consequently, PIPA does not apply to the Public Body and therefore the Public Body cannot be in breach of PIPA.

Does the *Maintenance Enforcement Act (MEA)* apply?

[9] The *Maintenance Enforcement Act* (MEA) contains a provision that prevails despite the FOIP Act (see section 5 of the FOIP Act and section 16 of the FOIP Regulation).

[10] However, the information at issue is information about employees of MEP. It is not information that was received by the Director of Maintenance Enforcement for the purposes of the administration of the maintenance enforcement program under the MEA.

[11] Therefore, the MEA does not apply to the information at issue in this investigation – the FOIP Act does.

IV. ISSUES:

[12] The issues for this investigation are as follows:

- Did the Public Body collect personal information in contravention of Part 2 of the FOIP Act?

- Did the Public Body use personal information in contravention of Part 2 of the FOIP Act?

- Did the Public Body disclose personal information in contravention of Part 2 of the FOIP Act?

V. INVESTIGATION FINDINGS AND ANALYSIS

The Maintenance Enforcement Program

[13] MEP is a program delivered by the Public Body. According to the Public Body's website, MEP is authorized by the MEA to collect child and spousal support payments and to forward these payments to the appropriate person. MEP has the legislative authority to take steps to enforce the support owed.[1]

[14] The Special Investigation Unit (the "SIU") in MEP is tasked with enforcing and collecting on complex files within the parameters of the MEA. The Public Body has an agreement with Equifax Canada ("Equifax"), under which MEP may access the Equifax database to obtain credit reporting services for legally permissible purposes.

[15] Access to the Equifax database is limited to certain SIU Staff. To obtain an individual's credit report, the following steps are taken by the SIU Staff:

1) Log into the Equifax database through a web browser using the required credentials.

2) Enter the individual's identifying information, such as their name, date of birth (DOB), and social insurance number (SIN).

3) View or print the individual's credit report.

[16] The credit report cannot be saved. After the SIU Staff exits the Equifax database, the individual's credit report is only accessible again after following steps 1 to 3.

[17] However, when an individual requests their credit report from Equifax, the credit report will list the credit inquiries conducted on that individual.

What Happened?

[18] In 2009, the SIU was conducting an "internal investigation" into allegations about fraudulent cheques being cashed at various locations. On December 22, 2009, MEP was able to ascertain that the breach was external, and handed the investigation over to a municipal police service. At that time MEP was able to state that the MEP cheques had not been compromised. However, this did not completely eliminate the possibility of internal involvement (by an employee) in the forgeries.

---

[1] From information published on the Public Body's website <http://justice.alberta.ca/programs_services/families/mep/Pages/default.aspx>

[19] To rule out the risk of internal involvement, MEP decided to obtain a credit report on all employees working in the Revenue Unit, and the Business Support Document and Initial Processing Unit. The task of obtaining the credit checks was assigned to a SIU staff (the "Peace Officer").

[20] An employee of the Public Body obtained the names, SINs and DOBs of the employees from records located at MEP's on-site personnel office. The list of names, SINs, and DOBs were sent in an email message to a Manager in the SIU ("the Manager"). The Manager then sent the email to the Peace Officer. [The Public Body was not able to confirm which employee was assigned the task of obtaining the information from the personnel records, or who sent the email to the Manager.]

[21] On January 18, 2010, the Peace Officer logged into the Equifax database and used the names, DOBs, and SINs of the employees to obtain the credit reports. The credit reports were printed on a printer accessible only to the Peace Officer. The Peace Officer said the credit reports were immediately hand-delivered to the Manager.

[22] The Manager gave the credit reports to the Director of Compliance. The Manager informed the Director of Compliance that the credit reports did not identify any potential risks. The credit reports were then provided to the Executive Director.

[23] The Public Body believes all credit reports were subsequently shredded. However, this cannot be confirmed as the Executive Director has since left the Public Body and it is unknown who shredded the credit reports or why these were shredded.

Public Body's Response

[24] The Public Body does not dispute credit checks were conducted on the employees. Further, the Public Body informed our Office:

> *"…the performance of the credit checks was inappropriate and in error…We will not be asserting any "technical" or legal defenses in response to these complaints. Rather, we would appreciate your guidance."*

[25] The Public Body said it has also taken steps to resolve this matter and to prevent a similar recurrence in the future (these steps will be outlined later in this report).

Did the Public Body collect, use or disclose personal information in contravention of Part 2 of the FOIP Act?

[26] Section 1(n) of the FOIP Act defines personal information as *"recorded information about an identifiable individual"* and would include an individual's name, address, SIN, DOB, and information about the individual's employment and financial history.

[27] The Public Body informed our office that a credit report would typically contain the following details about an individual: name, SIN, DOB, address, employer name, credit inquiries, judgments, past and present history of credit checks, credit rating, level of payments and updates.

[28] Consequently, when the Public Body obtained the credit reports, it collected personal information and that collection was subject to the FOIP Act.

[29] The Public Body said the performance of the "*credit checks was inappropriate and in error*". I have reviewed the circumstances and concur that the Public Body's collection of the Complainants' credit reports was not authorized under section 33 of the FOIP Act.

[30] As the Public Body was not authorized to collect the Complainants' credit reports in the first place, it would not be authorized to use that information under Part 2 of the FOIP Act. Further, the Public Body's use of the Complainants' personal information from the MEP personnel office to conduct the credit checks would also not be in accordance with section 39 of the FOIP Act.

[31] Some of the Complainants questioned whether the credit reports were disclosed outside the Public Body. The Public Body said the disclosure was limited to the Manager, the Director of Compliance and the Executive Director and I found no evidence that indicates otherwise.

Steps taken by the Public Body

[32] The Public Body said it has taken steps to resolve this matter and to prevent a similar recurrence in the future. I note the following steps in particular:

1. **Letter of Apology:** On May 19, 2010, the Deputy Minister sent a letter of apology to each employee whose credit report was likely obtained. In this letter, the Deputy Minister agreed to reimburse the employee for the expenses that were incurred as a direct result of the credit check.

2. **MEP on-site personnel records:** The Public Body has made a number of changes to provide better protection to employees' personal information that is kept in the personnel records located at the MEP on-site personnel office. MEP staff has confirmed to our office that MEP has worked closely with the Public Body's Human Resources Division to identify what employee information is appropriate to hold and track on-site at MEP. The necessary records have been identified and MEP has removed all extraneous records. The extraneous records were either shredded or sent to the appropriate file. As a result MEP not longer retains employees' SIN or commencement documents.

   In addition, the personnel records held by MEP are kept in a locked office, which is limited to three staff members who work with the records. Legitimate other access, such as access to previous performance assessments, is granted – however, removal of other documents is not permitted. Records are signed in and signed out.

3. **Scope and authority of Peace Officers:** The scope and authority of the Peace Officers is presently being defined more specifically to ensure their authority is utilized by MEP appropriately. MEP is in the process of framing a Standing Operating Procedure ["SOP"] that will outline the role of Peace Officers on employees and what they can and cannot do. This SOP will incorporate protocols to prevent Peace Officers from investigating Ministry employees in the future.

   In the interim (before the SOP is in place), Peace Officers have been told that they are not to investigate Ministry employees.

VI. CLOSING REMARKS

[33] I have completed my review of this matter. In my opinion, the Public Body did contravene Part 2 of the FOIP Act when it obtained the credit reports on the Complainants. The Public Body is in agreement that the credit checks on the Complainants should not have been performed.

[34] I believe the Public Body has taken reasonable steps to address the issues of this investigation and to prevent a similar recurrence. I also note that the Public Body has apologized to the employees who were affected by the credit checks. I have no additional recommendations to the Public Body.

[35] Lastly, I do not recommend that this matter proceed to an inquiry because there is no practical remedy that could be offered to the Complainants on this matter under the FOIP Act.

Submitted by

Veronica Chodak
Portfolio Officer, FOIP