

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

INVESTIGATION REPORT F2004-IR-003

**Report on Investigation into Complaint
Regarding the Security of Personal Information Collected
Pursuant to the Alberta Security Screening Directive**

December 10, 2004

**Alberta Personnel Administration Office
(Investigation #3136 and #3156)**

And

**Solicitor General
(Investigation #3137 and #3157)**

I. INTRODUCTION

[1] On November 10, 2004, the Commissioner was notified by the Alberta Government that documents containing personal information of a number of senior government employees had been found in a hotel room by the Edmonton Police Service during a credit card investigation. The documents related to the credit screening conducted by TransUnion of Canada Inc. ("TransUnion") as part of the Alberta Government's Security Screening Directive ("the Directive").

[2] Subsequently, the Commissioner received two written complaints from affected employees. The Commissioner's Office also received calls of concern from other affected employees who did not file formal complaints. The concerns communicated to the Commissioner's Office are summarized as follows:

- That the Personnel Administration Office (PAO) and Solicitor General did not follow the processes set out in the Directive and the promises made to employees regarding the retention and destruction of personal information collected pursuant to the Directive.
- That PAO and Solicitor General failed to protect the personal information submitted by employees and that this failure has placed employees at risk of identity theft and other fraudulent uses of their personal information.

[3] In response to the complaints received, the Commissioner authorized an investigation pursuant to section 53 of the *Freedom of Information and Protection of Privacy Act* ("the FOIP Act"). Under section 53(1)(a), the Commissioner may conduct

investigations to ensure compliance with any provision of the FOIP Act. Section 53(2)(e) allows the Commissioner to investigate complaints that personal information has been collected, used or disclosed in contravention of Part 2 of the FOIP Act. The Complainants and the Commissioner's jurisdiction under the FOIP Act frame this investigation.

[4] The investigation included meetings and interviews with representatives from the Edmonton Police Service, Solicitor General, and PAO. We also reviewed the documents found by the Edmonton Police Service and each of the security screening files at Solicitor General of the 507 employees who had completed the Level 2 screening process. This report sets out the findings and recommendations of our investigation.

II. APPLICATION OF THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

[5] The FOIP Act sets out the provisions under which public bodies may collect, use or disclose personal information. The FOIP Act also places a duty on public bodies to protect personal information against such risks as unauthorized access, collection, use, disclosure or destruction (section 38 of the FOIP Act).

[6] PAO and Solicitor General are separate public bodies under the FOIP Act. Therefore, the Commissioner opened the following files in response to the two formal complaints: #3136 and #3156 for PAO and #3137 and #3157 for Solicitor General.

[7] TransUnion is the credit bureau contracted by Solicitor General to conduct the credit screening for the Alberta Government. As a private sector organization, TransUnion is not a "public body" under the FOIP Act. However, section 1(e) of the FOIP Act reads:

1 In this Act,

(e) "employee", in relation to a public body, includes a person who performs a service for the public body as an appointment, volunteer or student or under a contract or agency relationship with the public body

[8] Under the FOIP Act, TransUnion is considered an "employee" of Solicitor General in relation to the credit screening information for provincial government employees since it has a contractual relationship with Solicitor General. However, the FOIP Act does not give the Commissioner jurisdiction over employees except through a public body.

III. BACKGROUND INFORMATION

[9] In 2002, the Deputy Minister's Committee, in consultation with the Public Service Commissioner, determined that a security screening process was desirable for the Alberta Public Service. The Directive embodies that screening process.

[10] As the corporate human resources agency for the Alberta Government, PAO was responsible for the development, implementation and maintenance of the Directive. The Security Services Branch of Solicitor General was responsible for liaising with the

agencies contracted to conduct the required security screenings. Solicitor General was also responsible for the retention and storage of the information obtained pursuant to the Directive.

[11] On September 13, 2002, the Public Service Commissioner wrote to all Deputy Ministers regarding the forms required under the Directive. All ministries were instructed to complete the forms for specific employees by September 19, 2002 and to submit these forms to the Security Services Branch at Solicitor General for processing.

[12] Information concerning the Directive was sent anonymously to the Commissioner on September 18, 2002. In response to the Commissioner's questions to the Public Service Commissioner, the security screening process was placed on hold pending further review. Forms that had already been received by Solicitor General were either retained at Security Services or returned to the respective ministries if requested. No processing was conducted on these forms.

[13] PAO subsequently submitted a Privacy Impact Assessment ("PIA") on the Directive to the Commissioner that outlined its authority to establish the Directive and the processes that would be implemented to safeguard the personal information submitted by employees in compliance with the Directive.

[14] The PIA outlined a number of changes from the initial instructions issued by PAO on September 2002:

1. The TransUnion Form would not be used to initiate the credit screening process.

Under the September 2002 instructions from PAO, employees were required to complete a TransUnion form ("the TransUnion Form") requesting a credit report. Solicitor General would then forward the TransUnion Form to TransUnion.

However, the TransUnion Form would have resulted in the Alberta Government collecting personal information about the employee that was not necessary for the credit screening process. The collection of personal information that is not related directly to and is necessary for an operating program or activity of a public body is a contravention of section 33(c) of the FOIP Act.

In addition, the purpose of the TransUnion Form was to request a credit report – it was not an authorization by the employee for the Alberta Government to collect the employee's credit information from TransUnion. The FOIP Act requires a public body to collect personal information directly from the individual the information is about unless it is authorized to collect from other sources, as set out in section 34 of the FOIP Act. Under section 34(1)(a)(i) of the FOIP Act, an individual may authorize a public body to collect the individual's personal information from another source.

The TransUnion Form was therefore replaced with the Financial Management Risk Indicator Screening Form. Unlike the TransUnion Form, the Financial Management Risk Indicator Screening Form did not require employees to provide

their Social Insurance Number (SIN), the years at their present address, and their previous address. The Financial Management Risk Indicator Screening Form also obtains the employee's consent and authorization for the credit screening.

2. The TransUnion Credit Reports would not be provided to the Alberta Government.

Initially, TransUnion was supposed to forward the employees' TransUnion Credit Report to Solicitor General. The TransUnion Credit Report contained more personal information than was necessary for the credit screening process. Therefore, the collection of the TransUnion Credit Report by the Alberta Government would have been a contravention of section 33(c) of the FOIP Act.

The Financial Management Risk Indicator Report was developed to reduce the amount of personal information collected by the Alberta Government. The Financial Management Risk Indicator Screening Form is a one-page document that contains the employee's name and a list of 10 financial risk indicators: bad debt write offs; paid collections; unpaid collections; bankruptcies; discharged from bankruptcy; ABM or bank frauds; active judgments; paid judgments; ratings above R2 or I2; and NSF cheques.

In the process described in the PIA, TransUnion would review the information contained in the TransUnion Credit Report in order to complete the Financial Management Risk Indicator Report. This requires TransUnion to simply mark either a "yes" or "no" on each indicator. The Financial Management Risk Indicator Report does not contain any details of the employee's financial and credit information. TransUnion then sends the completed Financial Management Risk Indicator Report to Solicitor General. The TransUnion Credit Report is not sent to Solicitor General.

3. An Alberta Government form would be used for the vulnerability risk indicator screening process.

The Canadian Security Intelligence Service (CSIS) was contracted to conduct the vulnerability risk screening for the Alberta Government. In the September 2002 instructions from PAO, employees were required to use the CSIS consent form. By replacing the CSIS form with the Alberta Government's Vulnerability Risk Indicator Screening Form, the amount of personal information required from employees is reduced.

[15] The Commissioner accepted the PIA on January 15, 2003. In accepting the PIA, the Commissioner acknowledged that PAO had the authority to make the Directive and that the ministries, boards, commissions and other entities under the *Public Service Act* had the authority to implement the Directive. However, the Commissioner cautioned:

"...this increased degree of scrutiny of employees also places an increased degree of responsibility on the employer in terms of getting accurate information, keeping it secure and using it for the purpose for which it was collected. I would regard any disclosure of this kind of information for any purpose other than that for which it was collected as a very serious breach of the law..."

[16] The security screening process for the Alberta Public Service was recommenced in February 2003.

IV. OVERVIEW OF THE DIRECTIVE

[17] The Directive applies to all ministries, boards, commissions, or other entities subject to the *Public Service Act*. The Directive requires security screening for all appointments or reclassifications to designated positions in the Alberta Public Service.

[18] Under the Directive, there are two security screening levels:

- Level 1 requires a criminal records check only.
- Level 2 requires criminal records check, financial management risk indicator check, and a vulnerability risk indicator screening.

[19] Level 2 applies to members of the Deputy Ministers Committee, members of ministry Executive Committees, Senior Financial Officers and other positions as determined by the ministry Deputy Minister in consultation with the Deputy Minister of Executive Council.

[20] The credit screening conducted by TransUnion is part of the financial management risk indicator check for the Level 2 screening.

V. INVESTIGATION FINDINGS

A. Documents Recovered by the Edmonton Police Service

[21] The Edmonton Police Service initially found documents containing the personal information of 43 provincial government employees. Subsequently, the Edmonton Police Service recovered documents containing information about an additional 185 provincial government employees.

[22] The initial documents found were: 14 completed TransUnion Forms, 29 Financial Management Risk Indicator Screening Forms and 43 TransUnion Credit Reports. The documents found subsequently included more TransUnion Forms, Financial Management Risk Indicator Screening Forms, TransUnion Credit Reports, fax cover pages between TransUnion and Solicitor General, and 220 completed Financial Management Risk Indicator Reports.

B. Personal Information Contained in the Documents

[23] The TransUnion Form contained the employee's name, address, years at present address, telephone number, SIN, date of birth and previous address (if current address is less than one year). As noted earlier, the purpose of the TransUnion Form is to request a credit report from TransUnion.

[24] The Financial Management Risk Indicator Screening Form (the Alberta Government form that replaced the TransUnion Form) contained the employee's name, previous surname, address, birth date, gender and signature.

[25] The TransUnion Credit Report included the employee's name, address, years at present address, home phone number, names of financial institutions, date of birth, and names of credit reports. The TransUnion Credit Report contained the employee's SIN if the employee had completed the TransUnion Form. However, if the employee had completed the Financial Management Risk Indicator Screening Form, the TransUnion Credit Report did not list the employee's SIN.

[26] Some of the TransUnion Credit Reports also included the employee's spouse's name and the spouse's employer. The TransUnion Credit Reports do not contain the employee's credit card numbers or bank account numbers.

C. Affected Employees

[27] A total of 507 employees underwent the Level 2 screening process. The police investigation recovered documents for 228 employees. Documents recovered contained fax dates ranging from February 2003 to December 2003.

[28] This Office was told that TransUnion destroyed all documents related to the credit screening process in its possession subsequent to the breach being publicly reported on November 12th, 2004. Since it cannot be determined which documents were lost and which were destroyed, it is unknown whether documents for the remaining 279 employees were also disclosed.

[29] This Office was informed that TransUnion wrote to all 507 employees:

"For your protection, we have placed a generic warning on your file. Placing this message on your file alerts credit grantors of your situation and recommends that they contact you before extending credit. This warning has proven to be an effective fraud protection tool and is widely recognized by credit grantors..."

D. The Location of the Breach

[30] The Edmonton Police Service say they don't know how the individuals charged in connection with the recovered credit information acquired the documents. However, based on the documents recovered by the police, this Office suspects the breach occurred from the TransUnion office in Edmonton and not from an office of Solicitor General or PAO.

- The TransUnion Forms and the Financial Management Risk Indicator Screening Forms all contain a fax header that gives the dates and times the documents were faxed from Solicitor General to TransUnion. Solicitor General says the method of transmitting these forms to TransUnion is via fax. This Office confirmed the original forms are in the security screening files at Solicitor General. The original forms do not have a fax header.

- According to the process established, TransUnion does not send the TransUnion Credit Report to Solicitor General. Other than 7 credit reports that were provided to Solicitor General directly by the employees, this Office confirms there were no credit reports in the security screening files at Solicitor General.
- Each TransUnion Credit Report recovered by the police does not display any fax header to indicate that these documents had been faxed from TransUnion to Solicitor General. Therefore, the TransUnion Credit Reports found appear to be originals, not copies.
- Each TransUnion Credit Report contains the date the report was generated (bottom right hand corner). The TransUnion Credit Reports were generated the same date or the following date as when the TransUnion Forms or Financial Management Risk Indicator Screening Forms were faxed to TransUnion. Therefore, it appears that these credit reports were generated in response to the forms that were faxed to TransUnion.
- The TransUnion Forms, the Financial Management Risk Indicator Screening Forms and the TransUnion Credit Reports initially found were stapled together according to the individual employee. While not all the documents subsequently found were stapled according to employee, the majority of the documents were.
- According to the process established, TransUnion faxes the completed Financial Management Risk Indicator Report to Solicitor General. The 220 Financial Management Risk Indicator Reports found by the police do not contain any fax headers. This would indicate that the Financial Management Risk Indicator Reports found were originals completed by TransUnion, not fax copies. This Office confirmed that faxed copies of the Financial Management Risk Indicator Reports are in the security screening files at Solicitor General. The faxed copies each have headers showing the dates and times when the documents were faxed from TransUnion to Solicitor General.
- A fax from Solicitor General to TransUnion listing 23 employees' names has a fax header that shows the date and time the document was faxed to TransUnion.
- Fax cover pages from TransUnion to Solicitor General have a "faxed" stamp, which is generally used by the office that is sending the fax, not the office that receives the fax.

E. The TransUnion Contract

[31] Although this Office believes that the documents found by the police originated from the TransUnion office, given the contractual relationship between TransUnion and the Alberta Government, the investigation reviewed the contract signed by TransUnion and Solicitor General. Our findings are as follows.

1. The decision to contract with TransUnion was made jointly by PAO and Solicitor General

[32] While Solicitor General signed the contract with TransUnion, the decision to engage and proceed with TransUnion was jointly made by Solicitor General and PAO. Therefore, both PAO and Solicitor General share responsibility in ensuring that TransUnion would safeguard personal information in relation to the credit screening process.

2. TransUnion sub-contracted to an agent.

[33] TransUnion's national headquarters is located in Toronto. TransUnion sub-contracted its Edmonton operations to Credit Information Services (PCS) Inc., a wholly owned subsidiary of Nor-Don Collection Network, which is a collection agency. The two companies shared offices.

[34] The fax cover pages from TransUnion to Solicitor General have both "TransUnion" and "Credit Information Services (PCS) Inc. Exclusive Marketing Agents for TransUnion of Canada" as the letterhead.

[35] In reviewing the Financial Management Risk Indicator Reports sent from TransUnion to Solicitor General, the majority of the fax headers identify the sender as "Credit Information" or "CIS". However, 44 of the Financial Management Risk Indicator Reports have fax headers that identify "NCN Edmonton" as the sender and a different fax number than the one for Credit Information Services (PCS) Inc. The email address of the contact person for TransUnion is: [individual's name]@ncn.ca.

[36] This raises a number of questions that needs to be addressed by PAO and Solicitor General, such as:

- Are the operations of Credit Information Services (PCS) Inc. and Nor-Don Collection Network separated?
- Was the contact employee an employee of Credit Information Services (PCS) Inc. or an employee of Nor-Don Collection Network?
- Could employees for both companies access the TransUnion Forms, the Financial Management Risk Indicator Screening Forms, the TransUnion Credit Reports, and the Financial Management Risk Indicator Reports? If so, what safeguards are in place to protect personal information from improper use or disclosure?

3. Neither PAO nor Solicitor General knew TransUnion sub-contracted the credit screening to an agent.

[37] PAO and Solicitor General say they were not aware that TransUnion sub-contracted the credit screening to another company when the contract was signed. In addition, Solicitor General and PAO did not know the company shared offices with another company.

[38] However, the TransUnion Form which was sent by PAO to the Deputy Ministers on September 13, 2002 has "TransUnion" on the upper left-hand margin and "Credit Information Services (PCS) Inc. Exclusive Marketing Agents for TransUnion of Canada" on the upper right-hand margin. The TransUnion Form clearly shows there is an agent relationship.

[39] The contract with TransUnion was signed on September 16, 2002. Therefore, information that an agent relationship existed between TransUnion and Credit Information Services (PCS) Inc. was before PAO and Solicitor General prior to the signing of the contract.

4. There were no contractual obligations placed on TransUnion to protect personal information

[40] The contract between TransUnion and Solicitor General is a standard TransUnion subscriber agreement. There are no provisions regarding TransUnion's obligations, as an "employee" of Solicitor General under the FOIP Act for the credit screening services, to protect personal information.

[41] The "FOIP Contract Manager's Guide" (December 2003), a publication produced by the Government and Program Support Services Division (formerly known as Information Management, Access and Privacy) of Alberta Government Services, states:

"...When contracts involve services dealing with personal information,...there are many factors that you must consider...It is the policy of the Government of Alberta that its departments, agencies, boards, and commissions (collectively referred to as "public bodies") take access to information, protection of privacy and records management requirements into account when considering these types of contracts..." (page 1)

[42] The Alberta Government policy that access and protection of privacy provisions be incorporated into contracts involving personal information was also referenced in the 1997 "Contract Manager's Guide to Freedom of Information, Protection of Privacy and Records Management in the Government of Alberta".

[43] Both the 1997 and 2003 publications state that contracts involving personal information should specify the obligations for a contractor to protect personal information:

"Where a contractor is collecting personal information on behalf of a public body, the contract must stipulate how the requirements of the Act will be met by the contractor or organization in regard to controls relating to the use, disclosure, security and retention and disposition of the personal information be collected." (1997 guide, Page 5)

"...each public body must protect individual privacy by applying sections 33 to 42 of the FOIP Act. Therefore, if the contract involves the collection, use or disclosure of personal information for a public body, you must ensure that contractors handling the personal information meet those privacy obligations." (2003 guide, page 22)

"The duty to protect personal information applies to everyone working under the contract. (2003 guide, page 23)

5. There were no assessments of TransUnion's operations or policies and procedures

[44] PAO and Solicitor General did not ask TransUnion to provide them with its policies and procedures regarding the protection and safeguard of personal information in its custody.

[45] In the PIA concerning the new Operator's License Design and Card Production Services Project, Alberta Government Services (AGS) included information regarding the contractor's security policies, procedures and measures such as clearance requirements of the contractor on its employees; how information is classified and secured; access controls; record destruction procedures; and procedures during emergencies. In our view, the approach taken by AGS should be considered a "best practice" in the kinds of information a public body may require from a contractor when contracting out services that involves personal information.

6. Legal and FOIP personnel for Solicitor General and PAO did not review the TransUnion contract

[46] Solicitor General did not review the contract with their legal services before signing it. PAO says it was provided with a copy of the contract but did not review the contract in detail since it was not signing the contract.

[47] Both Solicitor General and PAO did not involve their FOIP personnel in order to determine if there were any privacy implications with the contract.

[48] A review from their legal and FOIP personnel would have provided Solicitor General and PAO the opportunity to identify any legal or privacy issues prior to finalizing the contract with TransUnion.

F. Implementation of security screening not in accordance with the PIA

[49] This investigation found that the security screening was not implemented in accordance with the PIA. This resulted in personal information collected in contravention of the FOIP Act. Our findings are listed below.

1. A number of ministries used the TransUnion forms for the credit screening process.

[50] The PIA states the Financial Management Risk Indicator Screening Form is to be used for the credit screening process. The Financial Management Risk Indicator Screening Form replaced the TransUnion Form that was initially sent by PAO to the Deputy Ministers in September 2002. Therefore, the TransUnion Forms should not have been used by the ministries for the credit screening process.

[51] However, on January 16, 2003, PAO sent an e-mail to Deputy Ministers and Human Resources Directors that states:

“The Information and Privacy Commissioner has accepted the Privacy Impact Assessment on our Security Screening Directive...To ensure a consistent approach in implementation for Current Executive Committee members and Senior Financial Officers, please return the previously completed forms to them and let them know that if they wish to volunteer for the security screening they can resubmit their original form or complete the new form...”

[52] A number of ministries (including PAO) re-submitted the earlier completed TransUnion Forms. Solicitor General says PAO did not provide any direction to Solicitor General to not process the TransUnion Forms.

[53] The Edmonton Police Service recovered 60 completed TransUnion Forms. Our review of the security screening files at Solicitor General found additional completed TransUnion Forms.

[54] All TransUnion forms contained an employee’s SIN. Solicitor General says there are 104 SINs in its security screening files.

[55] While a SIN is commonly used for credit checks, it is unreasonable to require a SIN if the credit reporting bureaus do not (Investigation Report P2004-IR-001 [20]). Since TransUnion is able to generate credit reports without a SIN, then the employee’s SIN is not necessary for the credit screening process.

[56] Section 33(c) of the FOIP Act authorizes a public body to collect personal information only if that information relates directly to and is necessary to an operating program or activity of the public body. Our investigation finds that the collection of the employee’s SIN for the credit screening process is not authorized under section 33(c) of the FOIP Act.

2. A number of ministries used the CSIS forms for the vulnerability risk indicator screening process.

[57] The PIA states an Alberta Government form would be used for the vulnerability risk indicator screening process. The Alberta Government Vulnerability Risk Indicator Screening Form replaced the CSIS Form that was sent to the Deputy Ministers in September 2002.

[58] The CSIS Form required more information from employees than was necessary for the vulnerability risk indicator screening process. For instance, the CSIS Form required employees to provide information about their immediate relatives. Immediate relatives included the children, parents and siblings of the employee and the parents of the employee’s spouse. Employees were required to provide the relative’s name, relationship to the employee, place of birth, date of birth, address and employer.

[59] The employees were also required to provide information about character references (such as colleagues, peers and friends). Information included the character reference's name, address, relationship to employee, period that the person has known the employee, telephone number and position and business address.

[60] The PIA states the Alberta Government Vulnerability Risk Indicator Screening Form would be used and not the CSIS form for the vulnerability risk indicator screening process. However, as stated earlier in this report, PAO sent instructions to ministries on January 16, 2003 that employees may complete the new forms or re-submit the forms previously completed.

[61] The investigation found 88 completed CSIS Forms in the security screening files at Solicitor General. The CSIS Forms were completed by employees from various ministries, including PAO.

[62] It appeared that some employees were informed that the information regarding their relatives and character references for the CSIS Forms were not required. However, 31 of the employees who completed the CSIS forms did provide the information. Therefore, not all employees were made aware that this information was not required.

[63] Solicitor General says there was no direction or instruction from PAO to not use the CSIS forms for the vulnerability risk indicator screening process. By using the CSIS form, Solicitor General collected more personal information than is necessary or required for the vulnerability risk indicator screening process.

[64] Therefore, the collection of information regarding immediate relatives and character references is not authorized under section 33(c) of the FOIP Act.

G. Other Matters

1. Consent to CSIS

[65] The CSIS form contains its own consent and authorization statements, which are specific to the objectives and purposes of CSIS. The consent statement reads:

"Unless cancelled in writing by the applicant to the authorized security official, this consent form shall be valid for conducting the specified checks and/or investigation, including subsequent updating requirements of the Government Security Policy.

I, the undersigned, do consent to the disclosure of preceding information and its subsequent verification to the Government of Canada, the use of my photograph for identification purposes and the release of Section C of this form if required."

[66] Section C contains information relating to criminal convictions in and outside of Canada.

[67] Given the wording of the consent statement on the CSIS Forms, we are uncertain whether employees signing the CSIS Forms would be consenting to a broader use and disclosure of their personal information than the Alberta Government security screening process.

2. Credit Reports

[68] The Financial Management Risk Indicator Report Form provides the information necessary for the credit screening process. The TransUnion Credit Report provides more information than is necessary for the purpose of the credit screening. Consequently, the collection of the TransUnion Credit Report would not be authorized by section 33(c) of the FOIP Act.

[69] Employees are given the option to contact TransUnion directly for TransUnion credit report as opposed to having a Financial Management Risk Indicator Report Form completed and sent to Solicitor General. PAO says the collection of the TransUnion Credit Report from an employee is acceptable as the employee is voluntarily providing that information about themselves. However, if a public body does not have authority to collect that information under section 33 of the FOIP Act, it cannot collect the personal information even if the information is provided voluntarily.

[70] Our investigation found 7 credit reports in the security screening files at Solicitor General that were provided by the employees. As the credit reports contain more personal information than is necessary, we find the collection of the credit reports is not authorized under section 33(c) of the FOIP Act.

3. Identification Information

[71] Some of the security screening files at Solicitor General contain copies of driver's licences, birth certificates, citizenship cards, passports, Alberta Health Care Cards and Alberta Government picture IDs. One file contained a resume and wage documents.

[72] Solicitor General says these documents were provided by the ministries as part of the criminal record check process. In order to process a criminal record check, a ministry must verify the employee's identification. The form for the criminal record check asks the ministry to indicate which identification was reviewed, not provide a copy of the identification. Solicitor General says it had advised PAO that there is a need to clarify this requirement with the ministries but no action has been taken to date.

[73] As the identification information is not required by Solicitor General for processing the criminal record check, the collection of identification information is not authorized under section 33(c) of the FOIP Act.

4. Level II Security Screening Results

[74] The PIA states all security screening information is to be retained at Solicitor General. PAO says that ministries are told not to retain any security screening information themselves.

[75] When the Level II screening process is completed for an employee, Solicitor General provides the respective Deputy Minister of that employee with a copy of the certificate issued by the police and a copy of the Financial Management Risk Indicator Report Form (or a copy of the credit report if it had been provided by the employee). Solicitor General retains the original copies in its security screening files.

[76] Information regarding the vulnerability risk indicator screening process cannot be disclosed. Therefore, Solicitor General issues a stamp that indicates only that clearance was received from CSIS.

[77] Solicitor General says it is complying with directions from PAO in providing this information to the Deputy Ministers and that employees have authorized the disclosure of this information to their ministries.

[78] Solicitor General told this Office that some Deputy Ministers are uncertain as whether they should retain the security screening results. Therefore, there is a possibility that copies of the security screening results may be retained in some ministry personnel files, which is contrary to the PIA and what was communicated to employees.

[79] We note some ministries amended their Financial Management Risk Indicator Screening Forms to include authorization from the employee for the ministry to destroy the security screening information after a period of about 3 weeks from the date that the ministry received that information.

[80] It seems that the ministries' understanding on the retention and destruction of the security screening results is not consistent. This is a matter that needs to be clarified by PAO and communicated to Solicitor General and all ministries.

5. Copies of Documents found by Edmonton Police Service

[81] The Edmonton Police Service provided Solicitor General with copies of the recovered documents relating to government employees. Solicitor General says no copies of these documents have been made or distributed to the affected ministries. The one set of documents at Solicitor General is secured in a safe with access restricted to one individual.

VI. CONCLUSIONS AND RECOMMENDATIONS

[82] The investigation concludes:

1. The documents recovered by the Edmonton Police Service likely originated from the TransUnion office. There is no evidence that the breach came from a provincial government office.

2. PAO and Solicitor General did not fulfill their obligations to protect personal information as required by section 38 of the FOIP Act in the contract with TransUnion. The contract did not include protection of privacy provisions, as is the policy of the Government of Alberta.
3. PAO and Solicitor General did not review the security arrangements at TransUnion to ensure that personal information was protected against such risks as unauthorized access, collection, use, disclosure or destruction.
4. A number of ministries, including PAO, used the TransUnion Form and the CSIS form instead of the Financial Management Risk Indicator Screening Form and the Alberta Government Vulnerability Risk Indicator Screening Form. As a result, personal information was collected in contravention of the FOIP Act.
5. The collection of TransUnion credit reports from employees and the identification information for the criminal record check are not authorized under section 33(c) of the FOIP Act.

[83] We recommend that:

1. PAO and Solicitor General review the contract with TransUnion to ensure that privacy protection provisions and TransUnion's obligations to protect personal information are incorporated. The contract should also set out TransUnion's obligations to ensure that its employees and agents, who are working under this contract, comply with the terms and conditions related to the protection of privacy set out in the contract.
2. PAO and Solicitor General review the security arrangements at TransUnion to ensure personal information is protected from unauthorized access, collection, use, disclosure and destruction.
3. PAO and Solicitor General review the relationships between TransUnion, Credit Information Services (PCS) Inc., and Nor-Don Collection Network to determine whether there are any privacy implications or risks for unauthorized access, use, disclosure or destruction of personal information.
4. PAO and Solicitor General ensure that ministries use the Financial Management Risk Indicator Screening Form and the Alberta Government Vulnerability Risk Indicator Screening Form for the security screening process.
5. PAO and Solicitor General clarify and document what specific personal information in relation to the Directive is to be collected and retained by ministries and Solicitor General.
6. Personal information collected in contravention of the FOIP Act should be removed from the security screening files at Solicitor General.

VII. CLOSING REMARKS

[84] Having privacy protection provisions in a contract is not a guarantee that a privacy breach will not happen. However, a contract with privacy protection provisions is evidence that a public body has been diligent in meeting its obligations to protect personal information.

[85] The purpose of a PIA is to assist public bodies in identifying and assessing privacy implications and risks prior to embarking on a program or initiative. Considerable time and effort were spent in preparing the PIA on the Alberta Government Security Screening Directive. The decision to develop forms such as the Financial Management Risk Indicator Screening Form, the Financial Management Risk Indicator Report, and the Alberta Government Vulnerability Risk Indicator Screening Form was excellent and creative. These forms were specific to the requirements of the Directive and ensured that the personal information required by employees and collected by the Alberta Government was the amount that was necessary for the security screening processes and authorized under section 33(c) of the FOIP Act. Therefore, it is a concern that PAO, who developed the Directive, the Alberta Government forms, and the PIA, chose to use the TransUnion Form and the CSIS form. By doing so and in not ensuring that all ministries used the Alberta Government forms, personal information was collected in contravention of the FOIP Act.

Submitted by,

Marylin Mun
Team Leader, FOIP