ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-17

Loblaw Companies Limited

June 11, 2012

(Case File #P2091)

I. Introduction

[1] Under s. 34.1 of the *Personal Information Protection Act* ("PIPA"), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[2] On April 2, 2012, I received a report from Loblaw Companies Limited (the "Organization") of an incident involving the unauthorized access to or disclosure of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] The Organization is registered as an extra-provincial federal corporation in Alberta. The incident occurred in Manitoba and involved a wholly owned subsidiary of the Organization (the "Subsidiary").

[6] The Organization reported the incident involved the following information:

- A payroll database (the "Payroll Database") that contains the name and current Alberta address of a former employee of the Subsidiary. The balance of the information in the Payroll Database with respect to this former employee was collected in Manitoba. The Alberta address was information collected in Alberta and obtained by the Organization as a result of sending an employment verification letter to the former employee in Alberta.
- Records on a shared drive concerning a scholarship program ("Scholarship Records") for employees and family members containing the following information: name, address, social insurance number, scholarship amount, position, and relationship to employee if applicable.

[7] The Organization has operational control over the Payroll Database and the shared drive containing the Scholarship Records. The Subsidiary had access to the Payroll Database and the Scholarship Records.

[8] The Organization reported 12 Alberta residents were involved in the incident (the "Affected Individuals.") One record out of a total of 5687 records in the Payroll Database pertains to a resident of Alberta. Eleven records out of a total of 49 in the Scholarship Records pertain to Alberta residents as either current or former employees or family members of employees of the Organization.

[9] I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA and the personal information of the Affected Individuals qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[10] On April 4, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between April 4, 2012, and June 4, 2012.

[11] The circumstances of the incident as reported to me by the Organization are as follows:

- On March 15, 2012, the police contacted the Subsidiary.
- The police had received information that sometime around March 11, 2012, a former employee of the Subsidiary (the "Former Employee") allegedly offered personal information of the Subsidiary's colleagues to a third person during a criminal transaction. Allegedly, the third party intended to use the personal information for identity theft.
- The police indicated the information may not be credible.
- The Former Employee was employed by the Subsidiary for 5 months.
- The Former Employee's employment responsibilities involved access to the personal information.
- There is no current police investigation with respect to the alleged sale of the personal information.
- The Former Employee was criminally charged with theft of a Subsidiary laptop.
- It is unknown if any personal information was contained on the laptop.
- The laptop had internet access capability to the shared drive containing the Scholarship Records. Records show that the Former Employee did not access the shared drive after the final date of employment. The laptop has not been recovered.
- The Organization is unable to determine which records the Former Employee accessed specifically in the Payroll Database or the shared drive containing the Scholarship Records.
- The following steps have been taken with respect to the alleged incident:

    - Social insurance numbers are being removed from the shared drive.
    - A review of access rights and security and training measures is being conducted.
    - The laptop's hard drive will be remotely "wiped" if it connects to the Internet.

- The Organization notified the Affected Individuals of the alleged incident by letters sent between March 29, 2012, and March 30, 2012.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[12] In considering whether to require the Organization to notify the Affected Individuals, I am mindful of PIPA's purpose, legislative principles, and the relevant circumstances surrounding the reported incident.

[13] Pursuant to section 37.1 of PIPA, I have the power to require the Organization to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure." In determining whether or not to require the Organization to notify the Affected Individuals, I must consider if there is a "real risk of significant harm" to the Affected Individuals as a result of the incident.

[14] In order for me to require that the Organization notify the Affected Individuals, there must be some harm – some damage or detriment or injury – that could be caused to those Affected Individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[15] The Organization reported the type of harm that could result from the alleged incident is identity theft. It rated the harm as high.

[16] The name and Alberta address in the Payroll Database and the scholarship amount, employment position, and relationship to employee in the Scholarship Records is not, in my view, highly sensitive information. However, the social insurance number in combination with the name and address of Affected Individuals in the Scholarship Records is highly sensitive personal information. The type of harm that could result from unauthorized access or disclosure to this personal information is identity theft or fraud. In my view, this is a significant harm.

[17] In order for me to require the Organization to notify the Affected Individuals concerning the highly sensitive information in the Scholarship Records, there must also be a "real risk" of significant harm to the Affected Individuals as a result of the incident. This standard does not require that significant harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.

[18] The Organization has no evidence to substantiate the allegations in the information received by the police. Despite this, the Organization takes the position that all data accessible by the Former Employee may have been compromised. The Organization also recognized that it is possible that the allegedly stolen laptop contained personal information if the Former Employee stored this information while employed. There is also no evidence of this. Given the nature of the information and the alleged criminal element involved, the Organization submitted that if the personal information was accessed or disclosed by the Former Employee, there would be a real risk of significant harm to the Affected Individuals.

[19] In deciding whether there exists a "real risk" of significant harm in this case to the Affected Individuals, I considered the following factors:

- Some of the personal information in the Scholarship Records is highly sensitive and could be used for identity theft or fraud.

- The length of time the Former Employee had access to the personal information.
- The inability of the Organization to determine what information was accessed by the Former Employee and if the access was for an improper purpose.
- The police information allegedly identifies the Former Employee as offering personal information in the course of a criminal transaction.
- There is an allegation that the personal information was intended to be used for identity theft.
- The police information has not been corroborated by other evidence and is of questionable credibility.
- The Former Employee has been charged with theft of a Subsidiary laptop.
- The laptop was capable of capturing or copying personal information accessible during the employment of the Former Employee.

[20] In Breach Notification Decision 2011-ND-003, Commissioner Work decided that, despite the Organization's inability to confirm whether personal information in a folder that contained human resource information found on a shared drive was actually accessed, there was a possibility that sensitive personal information was viewed or copied. Given the sensitive data elements and the length of time the information was potentially exposed, Commissioner Work decided there was a real risk of significant harm to the affected individuals and required the organization to notify those individuals under section 37.1 of PIPA.

[21] In this instance, the only evidence of unauthorized access or disclosure of personal information is primarily based on evidence that may not be credible and is not corroborated. However, the alleged criminal involvement, both in the allegations with respect to the personal information and the theft of the laptop, in combination with the access privileges the Former Employee had to the personal information are also very relevant factors. Considering this evidence in combination with all of the other factors discussed above, I have decided that there is a real risk of significant harm to the Affected Individuals with respect to the Scholarship Records as a result of this incident.

V. Decision

[22] I require the Organization to notify the Affected Individuals with respect to the Scholarship Records in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[23] I understand that the Organization already notified those Affected Individuals by way of a letter on March 29, 2012. However, the notification provided does not meet the requirements of section 19.1 of the Regulation. Section 37.1 (1)(a) of PIPA gives me the power to require that the Organization notify individuals in a form and manner prescribed

by the Regulation. Therefore, I require the Organization to notify the 11 Affected Individuals with respect to the Scholarship Records in accordance with section 19.1 of the Regulation.

Jill Clayton
Information and Privacy Commissioner