ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-16

VALPAK OF CANADA LIMITED

May 17, 2013

(Case File #P2237)

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 January 8, 2013, Valpak of Canada Limited (Organization) provided notice of an incident involving the unauthorized access to 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 a corporation in Alberta. 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 was collected in Alberta.

[6] The Organization reported the incident involved a file that contained the following information about individuals:

- name,
- social insurance number, and
- employment start and end date (if applicable).

[7] This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On February 1, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between February 11, 2013, and April 25, 2013.

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

- On November 14, 2012, a United States Postal Inspection Service investigator contacted the Organization and informed it that an individual who had been temporarily employed by the Organization (Temporary Employee) had been indicted and charged with mail fraud.
- The Temporary Employee was employed by the Organization between June and September 2011.
- When the Temporary Employee was arrested, the file with the personal information at issue was in his possession.
- The file contained the personal information of 3057 individuals from Canada and the United States of America who were hired by or became owners of

Organization franchises prior to September 2011. Of the 3057, 63 were identified as individuals from Alberta (Affected Individuals).

- The Temporary Employee allegedly opened post office boxes in the United States using 28 employee names from the file.
- The Affected Individuals' names were not used to open the post office boxes.
- The Organization is conducting an internal review of practices and procedures to prevent a similar incident from happening again.
- All individuals in the file, including the Affected Individuals, were notified of the incident by a letter sent December 14, 2012.

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

[10] 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.

[11] 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.

[12] 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.

[13] The personal information at issue is highly sensitive. It includes the name and social insurance number of the Affected Individuals. The type of harm that could result from unauthorized access to or disclosure of the personal information in this instance is identity theft or fraud. In my view, these are significant harms.

[14] In order for me to require the Organization to notify the Affected Individuals, 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.

[15] The Organization reported the incident posed a low risk of significant harm. It confirmed that none of the Affected Individuals information was used to open the post boxes.

[16] Based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the Affected Individuals as a result of this incident. In my view, it is significant the Affected Individuals' highly sensitive personal information was in the possession of the Temporary Employee for a considerable period of time, between June 2011 and the date of the discovery of the fraud in November 2012. Another factor that contributed to my decision was the Temporary Employee was charged with fraud associated with use of personal information in the File.

V. Decision

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

[18] I understand the Organization notified the Affected Individuals in a letter sent on December 14, 2012. The December 14, 2012, letter is in accordance with the requirements of the Regulation. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner