ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-21

COLLEGE OF REGISTERED DENTAL HYGIENISTS OF ALBERTA

August 27, 2012

(Case File #P2130)

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 June 29, 2012, the College of Registered Dental Hygienists of Alberta (the "Organization") provided notice of an incident involving the loss 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 a "professional regulatory organization" under section 1(1)(k.2) of PIPA that is operating in Alberta. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The Organization reported the incident involved the following information of 15 of its employees:

- first and last name;
- home address;
- employment income for 2011;
- amount of income tax deducted from their income;
- employment insurance insurable earnings;
- employment insurance premiums;
- Canada Pension Plan pensionable earnings; and,
- social insurance number (SIN).

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

III. Background

[8] On July 24, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between July 24 and 26, 2012.

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

- The Organization contracts with an Accounting Firm ("AF") for the provision of accounting services.
- The AF prepared a T4 summary on the Organization's behalf. The T4 summary was placed into an envelope and mailed by the AF to the Canada Revenue Agency ("CRA") on January 27, 2012, by a receptionist (the "Receptionist") at the AF.

- On May 30, 2012, the CRA contacted the Organization and said that the CRA had not received the Organization's T4 summary.
- The Receptionist confirmed that the envelope was mailed on January 27, 2012.
- The Organization stated the T4 summary may have been misplaced within the offices of the CRA or lost by Canada Post. The envelope was sent by regular mail and could not, therefore, be tracked.
- The T4 summary has not been recovered.
- The Organization verbally notified the affected individuals of the incident between May 31 and June 21, 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 first and last name, home address, and social insurance number of the 15 affected individuals. The type of harm that could result from unauthorized access to 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 did pose a significant risk of harm to the affected individuals. The Organization indicated that the social insurance number combined with other information about an individual is enough for a dishonest person to potentially commit identity theft in relation to an individual.

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

- The personal information involved is highly sensitive and could be used to commit identity theft or fraud.
- The organization does not know if the envelope containing the T4 summary ever reached the CRA.
- The T4 summary has not been recovered.

[17] In Breach Notification Decisions P2012-ND-14 and P2012-ND-15, one of the factors I considered in determining that a real risk of significant harm existed to the affected individuals in those cases is that T4 slips, which include similar personal information as reported in this case, was lost and not recovered by the Organizations that experienced the breach.

[18] Based on the information reported to me by the Organization, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident.

V. Decision

[19] I understand that the Organization has notified the affected individuals in accordance with the Regulation. Therefore, I will not require the Organization to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner