ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-22

THE EQUITABLE TRUST COMPANY

August 17, 2012

(Case File #P2122)

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 18, 2012, The Equitable Trust Company (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 registered in Alberta as an extra-provincial trust corporation. The incident occurred in Toronto, Ontario. 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 original Guaranteed Investment Certificate ("GIC") application forms (the "Applications") of two Alberta residents (the "Affected Individuals"). The Applications contained the following information:

- name,
- address,
- social insurance number,
- investment details (issue and maturity dates, amount, term, rate, interest payment frequency), and
- identification information (birth certificate number and place of issuance for one Affected Individual and driver's licence number and issuing province for the other Affected Individual).

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

III. Background

[8] On June 21, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between June 25, 2012, and July 19, 2012.

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

- A GIC application of an Ontario client was retrieved from a garbage station in Toronto.
- Following this incident, the Organization conducted an investigation. The Organization discovered that an Organization employee may have disposed of other GIC applications in this manner.

- The Affected Individuals' Applications were not filed during the week of June 11, 2012. The Organization believes the Applications were also inappropriately disposed of by an Organization employee in residential garbage sometime between May 16, 2012, and May 22, 2012.
- The Applications have not been recovered.
- The Organization conducted an audit of security measures in place. The employee involved was sanctioned.
- The Affected Individuals were sent a letter during the week of June 18, 2012, with respect to the incident.

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 the 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. 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, this is a significant harm.

[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 recognized that if the Applications were retrieved by a third party, the information in the Applications is sensitive. There is no evidence the information was stolen or used for an inappropriate purpose.

[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 is highly sensitive.
- The Applications have not been recovered.
- The incident was caused by human error.

[17] Breach Decision P2011-ND-036 also involved highly sensitive personal information on a memory stick that was lost and not recovered. In that decision, Commissioner Work determined that the affected individuals were at risk for identity theft as a result of the incident. He decided in that case that the circumstances posed a real risk of significant harm to the affected individuals.

[18] 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.

V. Decision

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

[20] I understand the Organization sent a letter to the Affected Individuals with respect to the incident during the week of June 18, 2012, that is in accordance with the Regulation. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner