ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2010-ND-008

THE EQUITABLE TRUST COMPANY

November 22, 2010

(Case File #P1703)

I. Introduction

[1] On October 22, 2010, I received a report from The Equitable Trust Company (Equitable Trust) of an incident involving the loss of and possible unauthorized access to personal information of individuals. Based on the information reported to me, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that Equitable Trust notify those individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] Under section 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.

[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 signification 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) 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] Equitable Trust is a federally-incorporated trust company, registered under the Alberta *Loan and Trust Corporations Act* to operate in Alberta, and the incident at issue occurred in Alberta. I have jurisdiction in this matter because Equitable Trust qualifies as an "organization" pursuant to section 1(1)(i) of PIPA.

[6] The personal information at issue is that of Equitable Trust customers. This is information about identifiable individuals and so qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

[7] In considering whether to require Equitable Trust to notify affected individuals, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

[8] On October 22, 2010, I received a written report from Equitable Trust describing an incident involving the loss of, and possible unauthorized access to, personal information.

[9] On October 26, 2010, my Office contacted Equitable Trust to request additional information regarding this incident. Additional information was provided in telephone calls and through email correspondence from October 26-November 9, 2010.

[10] Equitable Trust reported to me that on or around October 19, 2010, a company-issued laptop assigned to an Equitable Trust employee was stolen from the backseat of the employee's car while it was parked overnight at the employee's home.

[11] The laptop contains personal information of Equitable Trust customers, which was included in email correspondence, and in file attachments to that correspondence.

[12] Equitable Trust reported that approximately 135 emails contained "sensitive" personal information. This information includes mortgage applications, name, address, Social Insurance Numbers (SINs), credit bureau reports, income, employer, payment history, telephone numbers, account numbers and mortgage balances.

[13] In addition, the personal information of approximately 2870 clients was included in various reports. This information includes the name, address, account number and mortgage balance for these individuals.

[14] The laptop requires a password to log on and obtain access; however, the personal information stored on the laptop was not in an encrypted format.

[15] Equitable Trust reported that, following this incident …

> *… steps were taken to mitigate any further damage including: locking the network/e-mail connectivity of the laptop to our servers such that no further data could be transmitted to the laptop and filing a police report. Additionally, we advised our employees that they are to be extra diligent in dealing with requests regarding Western clients."*

[16] To date, the laptop has not been recovered.

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

[17] Pursuant to section 37.1 of PIPA, I have the power to require Equitable Trust 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 Equitable Trust to notify individuals in this case, I must consider whether there exists a "real risk of significant harm" to those individuals as a result of the incident.

[18] In order for me to require that Equitable Trust notify individuals, there must be some harm – some damage or detriment or injury – that could be caused as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[19] With respect to the 135 emails that included mortgage applications, name, address, SINs, credit bureau reports, income, employer, payment history, telephone numbers, account numbers and mortgage balances, Equitable Trust reported that this information is "highly sensitive" and could "potentially be used to commit fraud and/or identity theft." Equitable Trust further stated that "[t]he combination of information varied from e-mail to e-mail however, we believe that such combinations increase the sensitivity."

[20] I agree with Equitable Trust that this personal information is highly sensitive, and could be used to cause significant harm to individuals, including identity theft and/or fraud.

[21] With respect to the information of the other 2870 customers that was included in various reports on the laptop, Equitable Trust reported that this information was "less sensitive" as it "was limited to the name, address, account number and mortgage balance" and therefore the potential risk of harm is significantly reduced. When asked to provide additional information about the "account number", Equitable Trust explained that the "account number" is …

> *… strictly an internal number set up by Equitable as an identifier for a loan. An individual having access to this number would not, consequently, have access to additional customer information. In addition, Equitable does authenticate all*

customers beyond name, address and loan number, prior to the release of any information.

[22] Considering the additional information provided by Equitable Trust, I agree with Equitable Trust's assessment that the personal information in this second category is of low to moderate sensitivity. While still of concern to me, this personal information could not reasonably be used to cause significant harm to individuals in the form of identity theft or fraud.

[23] With respect to the sensitive information in the 135 emails, however – which I believe could be used to cause significant harm to individuals – I must also consider whether there is a "real risk" of such harm in order for me to require Equitable Trust to notify these individuals. This standard does not require that harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm.

[24] In deciding whether there exists a "real risk" of harm in this case, I considered that Equitable Trust reported that there is "no specific evidence that information was [the] target of [the] theft," and that the laptop requires a password to log on and to obtain access.

[25] Despite these considerations, however, I have nonetheless decided there is a real risk of significant harm to the individuals in this case. The laptop was protected only by a logon password which is relatively easy to bypass. Further, it is significant to me that the laptop was stolen and not lost; the fact that the laptop was taken by someone who was, at the time, intentionally committing a criminal act, suggests that it is likely that the perpetrator(s) would have no compunction about using the personal information stored on the laptop to commit fraud or identity theft if the logon password were to be bypassed and the information was in fact accessed.

V. Decision

[26] Based on the information reported to me by Equitable Trust, I have concluded there is a real risk of significant harm to the customers whose personal information was included in the approximately 135 emails, and I require Equitable Trust to notify these individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation,* and confirm in writing to my Office that it has done so on or before December 8, 2010 or such other date as I may specify.

Frank Work, Q.C.
Information and Privacy Commissioner