ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-19

TAUCK, Inc.

July 23, 2012

(Case File #P2118)

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 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 May 24, 2012, TAUCK, Inc. (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 incorporated in the United States of America. The Organization operates in Alberta through Canadian subcontractors. The incident involved two Alberta residents (the "Affected Individuals") who booked a European travel tour (the "Tour") with the Organization through a travel agent located in Airdrie, Alberta. The incident occurred while the Alberta residents were on the Tour.

[6] The Organization reported the incident involved the following information with respect to the Affected Individuals:

- names, addresses, emergency contact information, and travel information (flight and hotel reservations). This information was contained on a laptop computer (the "Laptop Information").
- names, addresses, and departing flight information contained in guest information forms (the "Forms"). There were also fields in the Forms to collect passport information (passport number, issue date, place of issue, expiration date, nationality and place of birth) and health information (food allergies, medications and other medical issues the Tour Director should be aware of such as difficulty walking or climbing stairs).

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

III. Background

[8] On June 11, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between July 2, 2012, and July 18, 2012.

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

- The Affected Individuals were provided with the Forms on April 15, 2012, while on the Tour, in London, England.
- The Forms were returned to the Organization's Tour Director.

- The Forms were prepopulated by the Organization with the Affected Individuals' names, addresses and departing flight information.
- The Tour Director's briefcase was subsequently stolen in Paris, France.
- The Organization notified law enforcement of the theft.
- The briefcase and its contents have not been recovered.
- The briefcase contained the laptop and the original Forms.
- The laptop was password protected and encrypted. The laptop was remotely disabled. The laptop has not been used to connect to the Internet since it was disabled.
- The Organization does not have copies of the Forms. The Organization is unable to confirm if the Affected Individuals filled in the health information and passport information portions on the Forms.
- On May 21, 2012, the Organization sent a letter notifying the Affected Individuals about 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 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] With respect to the stolen laptop, the Laptop Information is of low sensitivity. In my view, there is no significant harm that could occur to an individual as a result of unauthorized access to this information.

[14] With respect to the Forms, even though the Organization cannot confirm that the Affected Individuals filled out the fields with respect to the passport and health information, it is reasonable that when presented with a form with fields that request this information, this information would be provided by the Affected Individuals.

[15] The extent or nature of the health information is not known. There is not enough information concerning the nature of the health information on the Forms to make an

assessment of the harm. The other information on the Forms, including the passport information is, however, highly sensitive.

[16] A representative of my Office consulted Passport Canada to determine what risk may be associated with the theft of a passport number. A Passport Canada representative indicated that a passport number without the official document cannot likely be used for immigration fraud. In my view, while the passport number without the document may not be useful from an immigration fraud perspective, it is identity information recognized in the *Criminal Code* of Canada that places an individual at risk for identity theft. [1] In my view, this is a significant harm.

[17] 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.

[18] The Organization reported the incident did not pose a real risk of significant harm to the Affected Individuals for the following reasons:

- The laptop was password protected and encrypted.
- The laptop was disabled shortly after learning of the theft.
- The Laptop Information was limited and of low sensitivity.
- The Forms requested very limited health information. It did not include sensitive information such as health insurance or treatment information.
- The Organization cannot confirm what, if any, health information or passport information was collected.
- With respect to the passport information on the Forms, the Organization contacted the U.S. State Department to discern what could be done with this information. The Organization understands that "it could not be used to facilitate identity theft." The May 21, 2012, letter from the Organization informed the Affected Individuals of this information.

[19] In my view, there is no real risk of significant harm to the Affected Individuals as a result of the theft of the Laptop Information. The Laptop Information is not sensitive and no significant harm could occur to the Affected Individuals as a result of unauthorized access to this information. Further, the laptop was password protected, encrypted and disabled shortly after the theft occurred.

[1] Section 402.1 of the *Criminal Code* includes "passport number" in a list of identity information that is commonly used alone or in combination with other information to identify or purport to identify an individual. Section 402.2(1) of the *Criminal Code* addresses the offence of identity theft. It is an offence to knowingly obtain or possess another person's identity information in circumstances that give rise to a reasonable inference that the information is intended to be used to commit an indictable offence.

[20] With respect to the information in the Forms, in deciding whether there exists a "real risk" of significant harm to the Affected Individuals with respect to the theft of this information, I considered the following factors:

- The information was stolen.
- The information has not been recovered.
- The nature of the health information provided on the Forms is unknown.
- It is likely that the passport information was provided on the Form by the Affected Individuals.
- The information on the Forms, along with the passport information, is highly sensitive.
- A "passport number" is recognized in the Criminal Code as being identity information that poses a risk for identity theft.

[21] Based on the above and given the circumstances of this incident, I have decided that there is a real risk of significant harm to the Affected Individuals with respect to the information on the Forms.

V. Decision

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

[23] The May 21, 2012, letter to the Affected Individuals met the Regulation requirements. Therefore, I will not require the Organization to re-notify the Affected Individuals with respect to the Regulation requirements.

[24] However, pursuant to section 37.1(2) of PIPA, I am, in addition to requiring notification pursuant to the Regulations, able to require an organization satisfy any terms or conditions that I consider appropriate. In accordance with this section, I require the Organization to notify the Affected Individuals with respect to the identity theft concern regarding the Forms and the passport number. This notification must be done on or before August 24, 2012. The Organization must also provide written notice to my Office that this notification has been done by that date.

Jill Clayton
Information and Privacy Commissioner