ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-27

UNIGLOBE GEO TRAVEL INC.

November 15, 2012

(Case File #P2142)

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 July 31, 2012, Uniglobe Geo Travel Inc. (the "Organization") provided notice of an incident involving the unauthorized access to or disclosure 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. 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 a database (the "Database") of approximately 1200 individuals (the "Affected Individuals"). The incident involved the following information:

- name of traveler, and
- credit card number and expiry date used to book the travel.

[7] The Organization reported that it could not confirm if the name of the traveler in the Database was the name of the credit card holder associated with the credit card number and expiry date. The name on the credit card used to book the travel may be different than the name of the person who traveled. The Organization acknowledged that the traveler name and the credit card holder name associated with the credit card number in the Database could be the same individual if the traveler used their credit card to book the travel.

[8] Information on a credit card is used to distinguish one individual from another in a commercial transaction. The credit card holder is identifiable by the traveler who used the credit card to book the travel. It is also more than likely that in most cases the traveler is the same as the credit card holder. This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[9] On September 5, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between September 10, 2012, and September 24, 2012.

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

- Between July 16, 2012, and July 23, 2012, an unauthorized person obtained an employee's login credentials by intercepting email sent on a wireless network. As a result, the unauthorized person gained access to the Database.
- The Organization is unable to identify which customers may have had their credit card number compromised. The Organization cannot confirm if the name of the traveler in the Database is the same as the credit card number holder.
- Police were notified of the incident on July 24, 2012.
- All employees who are users of the Database changed their login credentials.
- All servers and desktops were scanned for malicious malware.
- An IT specialist has been retained to review the infrastructure and security protocol.
- Since the Organization cannot identify with certainty the card holder name associated with the credit card number in the Database, the Organization sent an email message to the entire customer database of 2700 individuals with respect to the incident on July 24, 2012.

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

[11] 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.

[12] 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.

[13] 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.

[14] The personal information at issue is of high sensitivity. 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.

[15] 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.

[16] The Organization reported the incident did not pose a significant risk of harm since the traveler name may or may not have been associated with the credit card number and expiry date. The Organization also did not believe there was a real risk of harm since the Database did not include the security number for the credit card.

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

- The Database involves personal information of high sensitivity.
- Unauthorized access to the Database could result in identity theft or fraud.
- The unauthorized access involved malicious intent.
- The number of Affected Individuals and the inability of the Organization to accurately identify the card holders with the credit card numbers and expiry dates in the Database.
- The likelihood that the name of the traveler is also the individual uniquely associated with the credit card information in the Database.

[18] In Breach Decision P2011-ND-001, name, credit card number, expiry date and car rental information was compromised by keystroke logger malware. Some credit card numbers were used for fraud. The compromised information in this case did not include the security number for the credit card. In Breach Decision P2011-ND-26, a virus resulted in the compromise of credit card information, internet password and website login information for certain employees. In both decisions, Commissioner Work decided that there was a real risk of significant harm, due to the circumstances and the sensitivity of the information, and required the organizations to notify the Affected Individuals.

[19] 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

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

[21] I understand that the Organization sent an email on July 24, 2012, to all 2700 customers that included the Affected Individuals in accordance with the Regulation. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner