ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-25

OANDA (Canada) Corporation ULC

September 19, 2012

(Case File #P2135)

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 19, 2012, OANDA (Canada) Corporation ULC (the "Organization") provided notice of an incident involving unauthorized access to personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to the individual as a result of the incident. I require that the Organization notify the individual 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. The incident involved an employee's computer located at the Organization's head office 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 incident involved three account holders. One account holder is an Alberta resident (the "Affected Individual"). The Organization reported the incident involved the following information:

- name,
- address,
- email address,
- passport number,
- passport issue and expiry dates,
- citizenship,
- date of birth,
- employer name,
- self-declared annual income and net worth amounts, and
- account balance

(the "Account Information").

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

III. Background

[8] On August 13, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization on the same date.

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

- The Organization provides an online foreign currency trading platform service to account holders.
- The Organization investigated a report by an account holder on July 17, 2012, of unusual activity in his or her account.
- The Organization discovered a head office employee's computer was hacked between July 14, 2012, and July 17, 2012.
- Audit records show that the hacker gained access to the customer database and viewed the Affected Individual's Account Information.
- The incident was reported to the police. The hacker is unknown.
- The Organization notified the Affected Individual of the incident by email on July 18, 2012.
- The Affected Individual acknowledged receipt on July 24, 2012, of the email notification of the incident and changed his or her authentication credentials.

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 Individual, 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 Individual, I must consider if there is a "real risk of significant harm" to the Affected Individual as a result of the incident.

[12] In order for me to require that the Organization notify the Affected Individual, there must be some harm – some damage or detriment or injury – that could be caused to the Affected Individual 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 of high sensitivity. The type of harm that could result from unauthorized access to the Account Information in this instance is identity theft and fraud. In my view, these are significant harms.

[14] In order for me to require the Organization to notify the Affected Individual, there must also be a "real risk" of significant harm to the Affected Individual 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 the nature of the Account Information and the circumstances of the incident did pose a risk for identity theft to the Affected Individual. However, the Organization assessed the risk as low because the passport number was

expired at the time of the incident, no other sensitive information such as social insurance number was involved, and no unauthorized activity had occurred in the Affected Individual's account.

[16] A passport number, in addition to date of birth, is identity information recognized in section 402.1 of the *Criminal Code* of Canada (the "Code"). Section 402.2(1) of the Code is the identity theft offence provision. If identity information is in the possession of an individual where a reasonable inference may be made that it may be used to commit an offence, this may constitute an offence under that section. [1]

[17] A representative of my Office consulted Passport Canada to determine if a passport number would change if a passport had expired and a new one was issued. Passport Canada indicated that a passport number would change if a new passport was issued.

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

- The amount and type of personal information accessed by the hacker is highly sensitive and could be used to commit identity theft and fraud.
- The passport had expired at the time of the incident and the passport number would not be reissued.
- The Account Information was accessed by a hacker, possibly for nefarious purposes.

[19] The circumstances of this incident are similar to those in Breach Decision 2012-ND-02. In Breach Decision 2012-ND-02, an organization's database was hacked. The personal information accessed included name, address, date of birth, income information and the last three digits of a social insurance number. Due to the sensitivity of the information involved and the circumstances of the incident, I decided the incident posed a real risk of significant harm and required the organization to notify the affected individual.

[20] This incident involves an expired passport number that, similar to a partial social insurance number, may be of limited use. However, even with an expired passport number, the balance of the Account Information was highly sensitive and was accessed by a hacker likely with malicious intent.

[21] 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 Individual as a result of this incident.

[1] Section 402.2(1) of the *Criminal Code* states that 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.

V. Decision

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

[21] I understand that the Organization has notified the Affected Individual in accordance with the Regulation in an email sent on July 18, 2012. Therefore, I will not require the Organization to notify the Affected Individual again.

Jill Clayton
Information and Privacy Commissioner