ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-24

Oil City Hospitality Inc.

September 28, 2012

(Case File #P2127)

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 26, 2012, Oil City Hospitality 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 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 the following payroll information (the "Payroll Information") of current and former employees:

- name,
- address,
- birthdate,
- social insurance number,
- start and end date (if applicable) of employment,
- rate of wage, and
- position.

[7] The Payroll Information pertained to 2100 employees from nine Organization establishments. Eight were located in Alberta (1950 employees) and one was located in British Columbia (150 employees).

[8] The Payroll Information of the 1950 former or current employees from the eight Organization establishments located in Alberta (the "Affected Individuals") qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[9] On July 10, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between July 16, 2012, and August 24, 2012.

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

- the Organization's head office in Edmonton, Alberta, was broken into sometime during the weekend of June 23, 2012.

- On June 25, 2012, the Office Manager discovered that a memory stick was missing from her desk. The memory stick appeared to be the only item stolen.
- The memory stick contained the Payroll Information for a three-year period. The memory stick was the backup to information on the Office Manger's hard drive.
- The memory stick was not password protected or encrypted.
- The Organization reported the incident to the police.
- A letter was sent to the last known address of the Affected Individuals with respect to the incident on June 25, 2012 (the "Letter").
- Out of a total of 2100 Letters sent, a total of 253 have been returned to the Organization.
- The Organization is able to identify 100 Affected Individuals from Alberta who did not receive the Letter out of the 253 returned Letters.
- The Organization is unable to determine if 153 of the returned Letters pertain to Alberta or British Columbia employees. The Letters in the returned envelopes were not individually addressed. In addition, Canada Post placed a return sticker over the addressee information on these returned envelopes making it impossible for the Organization to read the addressee underneath.
- In addition to mailing the Letters, a copy of the Letter was posted on staff bulletin boards. As well, Managers at each establishment sent out an email to all current employees and posted about the incident on social media.
- The Organization installed additional physical security measures and would place passwords on data files.
- The Payroll Information has not been recovered.

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 highly sensitive. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft and 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 recognized in the report that the incident posed a high risk of identity theft to the Affected Individuals.

[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 Payroll Information contained on the memory stick is highly sensitive.
- A large number of current and former employees are involved.
- The memory stick was not password protected or encrypted.
- The memory stick was the only item stolen from an office. The circumstances of the theft increase the likelihood the Payroll Information will be used for nefarious purposes.
- The memory stick has not been recovered.

[18] In Breach Decision P2011-ND-2012, a memory stick containing sensitive personal information, including name, address and social insurance number, was lost and not recovered. The memory stick was not encrypted. Commissioner Work decided there was a real risk of significant harm to the affected individuals due to the sensitivity of the information and the risk with respect to identity theft and required the Organization to notify those 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 the Organization sent a Letter on June 25, 2012, to the Affected Individuals with respect to the incident. I will not require the Organization to directly re-notify all of the Affected Individuals.

[22] However, with respect to the 253 Affected Individuals that the Organization does not have valid contact information for or cannot identify the addressee on the returned Letters, I have determined that it is unreasonable in the circumstances to require the Organization to directly notify those Affected Individuals. I require the Organization to

notify in accordance with the Regulation the 253 Affected Individuals indirectly in the following manner:

a) post the notification on its establishments' websites for a period of 30 days, and

b) place the notification for a reasonable period in two major daily newspapers in Edmonton and Calgary.

[23] I require the Organization to confirm in writing to my Office that it has notified the Affected Individuals in accordance with the requirements set out above on or before October 17, 2012, or such other date as I may specify.

Jill Clayton
Information and Privacy Commissioner