ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-29

BP CANADA ENERGY GROUP ULC

November 8, 2012

(Case File #P2157)

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 August 27, 2012, BP Canada Energy Group ULC (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 information:

- full name,
- contact information (home address, alternate address if applicable, phone number),
- personal details (marital status, gender, birthdate, emergency contact information),
- social insurance number,
- compensation information (annual compensation amount and rate, compensation frequency, hire and last day worked dates, termination date (if applicable), professional experience date used to calculate benefits, service date, annual benefit base rate),
- 2010-2011 performance ratings, and
- payroll, timekeeping and status information (employee identification number, payroll direct deposit information, full or part-time status, union status, salary administration plan, annual benefit base rate, full time equivalent percentage, active or inactive status, full or part time status, salary or hourly employee.

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

[8] The balance of the information reported by the Organization was generated solely in relation to the employment position and is not personal information. This information includes job title, grade level, supervisor name and identification, internal codes and identifiers (salary administration plan, department identification, employee class, pay group, tax location, and work group).

III. Background

[9] Additional information was provided by the Organization between September 11, 2012, and September 21, 2012.

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

- On July 23, 2012, an employee of a subsidiary of the Organization discovered a laptop was stolen from their residence in Malaysia.
- The subsidiary employee used the laptop in connection with a project involving the transfer of data from the Organization's human resource management system to a new payroll system (the "Project").
- The laptop contained the personal information of approximately 2700 current, former or retired employees of the Organization (the "Affected Individuals").
- The subsidiary informed the Organization of the incident on August 16, 2012.
- The laptop was password protected. It was not encrypted.
- The theft was reported to the local law enforcement authorities in Malaysia.
- The laptop has not been recovered.
- The Organization implemented steps to ensure compliance with company policies and procedures regarding the storage and use of personal information on the Project.
- A letter notifying Affected Individuals of the incident was mailed on September 13 and 14, 2012.
- One year identity and fraud theft monitoring services were offered to the Affected Individuals. A dedicated telephone number was set up for Affected Individuals who have questions with respect to the incident.

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 in combination is of high sensitivity. 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 reported the incident poses a high risk of harm with respect to identity theft because the laptop was not encrypted. The laptop was stolen and has not been recovered.

[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 personal information is of high sensitivity and poses a risk of identity theft or fraud.
- The laptop was not encrypted.
- The laptop was stolen.
- The laptop has not been recovered.

[18] 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

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

[20] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in a letter sent between September 13 and14, 2012. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner