ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-34

ConocoPhillips Canada (North) Limited

January 7, 2013

(Case File #P2185)

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 October 31, 2012, I received a report from ConocoPhillips Canada (North) Limited (the "Organization") 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 the affected 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 as a federal corporation. 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 of 11 university students who applied for employment with the organization:

- Resumes, including student name, contact information (address, telephone number(s), email address), description of work experience, program of study and expected graduation date, biographical information (volunteer activities, computer skills, and scholarships, diplomas and other interests).

- University of Alberta "unofficial records," including student name, identification number, month and day of birth, program of study, courses taken, and grades

- Recruiting questionnaires, including student name, degree sought and date, grade point average, school attended, and responses to questions about the student's knowledge and experience, motivations, competencies, reasons for career choice, hobbies, etc.

- An interview matrix form listing the first name of all 11 students, each student's numerical score issued by the interviewer, and a notes section containing additional information about qualifications of each student if requested by the interviewer.

[7] In addition to the above, one student resume listed names and contact information for three references.

[8] The information described above for the 11 students and three named references qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[9] On October 30, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization on December 12 and 13, 2012.

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

- On October 17, 2012, an employee of the Organization had his or her house broken into.
- A workbag was stolen from the employee's house along with electronic items, a purse, wallet and several other small items of personal property.
- The documents containing the information described above were in the workbag when it was stolen.

- The theft was reported to the police.
- The documents have not been recovered.
- The students were notified about the breach on October 31, 2012, by email.

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 whether 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 the Organization to 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 be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[14] The Organization reported that the information contained in the documents is not highly sensitive. The Organization also reported that there is not a substantial risk of identity theft in this case.

[15] I first considered the information at issue for the three individuals named as one student's references. For these individuals, the only information involved in this incident is name and contact information. This information is of low sensitivity. In my view, no significant harm can occur to these individuals as a result of this incident. Given that the first part of the test of requiring notification – that the incident could result in significant harm to individuals – is not met, I do not need to decide whether there is any "real risk" of significant harm to these individuals.

[16] The personal information at issue for the 11 students, however, is of moderate sensitivity and could be used to cause significant harm. While each data element alone may not necessarily be sensitive, the combination of personal information could reasonably be used to cause significant harm in the form of identity theft and fraud. Further, the detailed interview information contained in the questionnaire as well as the scoring information in the interview matrix form could result in embarrassment, hurt and humiliation. In my view, these are significant harms.

[17] In order for me to require the Organization to notify the students, there must also be a "real risk" of significant harm occurring 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 harm to the students for the following reasons:

- The personal information is not highly sensitive.
- There is nothing to indicate the personal information was the target of the theft.
- The workbag was taken "for its own sake", not for the contents.
- There is no indication of any connection between the students and the thief.

[19] In deciding whether there exists a "real risk" of significant harm to the students, I considered the following factors:

- The amount and type of personal information involved in the incident.
- In combination the personal information is moderately sensitive and could be used to cause identity theft, fraud, embarrassment, hurt, and humiliation.
- The information was stolen and the documents have not been recovered.

[20] In P2012-ND-13, I decided there was a real risk of identity theft or fraud to individuals when their personal information, which was stored on an unencrypted flash drive, was lost. The personal information involved in that case was student name, birthdate, gender, student identification number, program of study, and grant information. In that case I stated the following:

> In my view, the personal information at issue in this case is of moderate sensitivity and could be used to cause significant harm to individuals. While name and date of birth alone may not necessarily be sensitive, when combined with other personal information elements, this is information that could reasonably be used to cause significant harm to individuals in the form of identity fraud or other financial fraud.

[21] Further, the incidents described in P2011-ND-005, P2012-ND-29, P2012-ND-01, and P2012-ND-08 all involved thefts of moderately to highly sensitive personal information. In each of these cases, the information was not recovered and it was decided there was a real risk of significant harm to the affected individuals.

[22] In my view, the information at issue in this incident, in combination, is moderately sensitive. The information was stolen, and has not been recovered. This personal information could reasonably be used to cause significant harm to the students in the form of identity theft, fraud, embarrassment, hurt and humiliation.

[23] Based on the information reported to me by the Organization and the foregoing, I have decided that there is a real risk of significant harm to the students as a result of this incident.

V. Decision

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

[25] I understand that the Organization has notified the students in accordance with the Regulation in an email sent on October 31, 2012. Therefore, I will not require the Organization to notify them again.

Jill Clayton
Information and Privacy Commissioner