ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-26

Technip Canada Limited

October 24, 2012

(Case File #P2138)

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 27, 2012, Technip Canada Limited (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 the personnel files of 24 employees and contractors (the "Affected Individuals"). The personnel files included the following information:

- offer letter or employment contract that includes name, date of birth, home address, phone number, email address, work permit or social insurance number, terms of employment,
- copies of educational or training certificates,
- new hire check list, and
- employee requisition form.

[7] The information contained in the offer letter, employment contract, and the educational or training certificates qualifies as "personal information" as defined in section 1(1)(k) of PIPA. Based on the description provided by the Organization, the new hire check list and the employee requisition form are not "personal information" as they relate broadly to the employment position and are not about identifiable individuals.

III. Background

[8] On August 22, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between August 30, 2012, and September 12, 2012.

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

- On July 26, 2012, the Organization discovered the Organization's personnel files were missing from a locked file cabinet.
- The personnel files were located in a locked file cabinet in an office in the Organization's premises located in a secured building. The building and the

Organization's office are accessible by an authorized I-disk key provided to authorized employees and contractors.

- The Organization believes the incident occurred sometime between the end of office hours on July 25, 2012, and the early hours of July 26, 2012.
- The personnel files were the only items missing.
- The Organization reported the personnel files as stolen to the police.
- The personnel files were found in the hallway outside the Organization's entrance in a secure building on July 27, 2012.
- On July 26, 2012, the Affected Individuals were informed of the incident at a staff meeting. The Organization also sent an email describing the contents of the personnel files on the same date.
- The Organization also sent a letter regarding the incident to the Affected Individuals on July 27, 2012, and updated them with respect to the recovery of the personnel files.

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

[12] 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.

[13] The Organization reported the incident posed a high risk of harm with respect to identity theft. It also reported a moderate risk of harm with respect to physical harm and home security since home addresses were found in the personnel files.

[14] The personal information at issue is of high sensitivity. The type of harm that could result from unauthorized access to or disclosure of the personal information in this instance is identity theft or fraud. In my view, these are significant harms.

[15] I am unable to assess the physical harm or home security concerns reported by the Organization based only on information that the home addresses were contained in the personnel files and the circumstances of the removal of the files from the office.

[16] 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.

[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 personnel files contained personal information of high sensitivity.
- The personal information could be used to commit identity theft or fraud.
- The personnel files were reported to the police as stolen.
- It is unclear what was done, if anything, with the personnel files, while they were missing or during the time they were unsecured in the hallway outside the Organization's office.

[18] In Breach Decisions P2010-ND-009 and P2012-ND-010 the lock to a file cabinet containing client files of two psychologists was tampered with. Some files appeared to have been moved. None were missing. In that decision, Commissioner Work decided due to the sensitivity of the personal information in those client files and based on the unusual circumstances, that the information was accessed by an unauthorized individual with the intent to cause harm. As a result, he required the organization to notify the affected individuals.

[19] Breach Decision P2012-ND-17 involved suspicious and alleged criminal circumstances with respect to the possible disclosure of sensitive personal information by a former employee. It could not be confirmed that the former employee accessed the personal information for an improper purpose. I decided, based on the circumstances and the nature of the personal information, that there was a real risk of significant harm and required the organization to notify the affected individuals.

[20] 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

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

[22] I understand that the Organization notified the Affected Individuals verbally, by email on July 26, 2012, and by a letter sent on July 27, 2012, in accordance with the Regulation. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner