ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-038

TECK COAL LIMITED

November 30, 2011

(Case File #P2016)

I. Introduction

[1] On October 25, 2011, I received a report from Teck Coal Limited ("Teck" or the "Organization") of an incident involving the unauthorized disclosure of personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that Teck notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] 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.

[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] I have jurisdiction in this matter because Teck is an "organization" as defined in section 1(1)(i) of PIPA, and the information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k).

[6] In considering whether to require Teck to notify affected individuals, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

[7] On October 25, 2011, I received a written report from Teck describing an incident involving the unauthorized disclosure of personal information.

[8] On October 31, 2011, my Office contacted Teck to request that it provide additional information concerning the incident, in order for me to determine whether to require Teck to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls, e-mail and mail correspondence between October 31, 2011 and November 28, 2011.

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

- The breach is the result of an incident where annual pension statements for some Teck employees were mailed to the wrong Pension Plan Members.
- The breach was the result of an incorrect data sort on an excel file which caused members' names to line-up with incorrect addresses.
- The incident occurred on July 7, 2011 and was discovered on July 13, 2011 when a Teck employee gave his foreman an unopened Annual Pension Statement envelope. The foreman subsequently provided the envelope to an individual in employee relations at Teck.
- There are 146 Teck employees who were affected by this breach. Teck reports that it sent out a total of 310 Annual Pension statements. The post office returned 145 of those 310 statements back to Teck, which leaves a total of 165 statements still unaccounted for. A further 19 of the 165 remaining statements were returned

by employees to the Teck Human Resources department. This leaves a total of 146 statements that have not been returned.

- The personal information at issue includes:
    - Name;
    - Birthdate;
    - Date of employment;
    - Date of registration;
    - Date vested;
    - Designated beneficiary and relationship;
    - Spousal birthdate;
    - Pension income amounts;
    - Employee number; and,
    - Retirement date.
- Notice was posted and some employees were advised orally following the incident. New pension statements were issued to employees on July 18, 2011 which included notification regarding the incident.
- In an effort to prevent this type of incident from occurring again, Teck has advised its employees that future pension statements will be mailed out in windowed envelopes. Additionally, e-mail communication has gone out to management advising that they double check information when distributing personal information to Teck employees.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[10] Pursuant to section 37.1 of PIPA, I have the power to require Teck 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 Teck to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

[11] In order for me to require that Teck notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the employees as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[12] In this case, the personal information at issue is of moderate sensitivity for the Teck employees as it includes name, birthdate, and pension information. The personal information involving the name of the employee's beneficiary is, however, highly sensitive given that the disclosure of this information can cause harm or humiliation to the employee. For example, should an individual be married, but not have his or her spouse designated as a beneficiary, knowledge of this as a result of the breach could cause the type of harm described.

[13] Teck also noted that the type of harm that could result from the unauthorized disclosure of this information is identity theft in addition to hurt, humiliation, and damage

to reputation, which, in my view, are significant harms. Teck did not, however, note whether or not there was a low, medium, or high risk of such harms potentially occurring as a result of the breach.

[14] In order for me to require Teck to notify its employees however, there must also be a "real risk" of significant harm to the employees 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. Further, there must be a cause and effect relationship between the incident and the possible harm.

[15] In deciding whether there exists a "real risk" of significant harm in this case, I considered that while the personal information at issue is of moderate sensitivity, it could be used to cause identify theft, which is a significant harm. In addition, the employee's beneficiary, considered as highly sensitive information, was included on the statements mailed in error, which could also result in a significant harm to an individual. In addition, I considered that there were 146 individuals (Teck employees) affected by the breach, and it is unknown at this point where the 146 pension letters are. The organization did instruct the affected employees to either destroy the information they received in error, or return it to the Teck employee relations department; however, following that posting, no letters were returned and Teck did not require employees to verify they had destroyed the statements received in error.

[16] Given the information reported by Teck, I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the following factors: the type of information involved could be used to commit identity theft or cause humiliation to the affected individuals; and, 146 pension statements were not returned to Teck nor was written confirmation of their destruction required.

V. Decision

[17] Based on the information reported to me by Teck, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Teck to notify the affected individuals. I understand Teck has already notified the individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of letter sent on October 27, 2011; therefore I will not require Teck to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner