

ALBERTA
OFFICE OF THE INFORMATION AND
PRIVACY COMMISSIONER

P2011-ND-006

TRANSALTA CORPORATION

February 22, 2011

(Case File #P1762)

I. Introduction

[1] On February 1, 2011, I received a report from TransAlta Corporation (“TransAlta” or the “Organization”) of an incident involving the loss 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 TransAlta 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 TransAlta 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 TransAlta 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 February 1, 2011, I received a written report from TransAlta describing an incident involving the loss of personal information.

[8] On February 7, 2011, my Office contacted TransAlta to request that it provide additional information concerning the incident, in order for me to determine whether to require TransAlta to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls between February 7, 2011 and February 9, 2011.

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

- TransAlta had retained a third party service provider, Workplace Safety & Healthcare Services Ltd. (“WSHS”) to perform clinic and on-site audiometric testing for employees at its Southern Alberta wind and hydro facilities.
- On November 23, 2010 WSHS was on-site at the Pincher Creek location and following the testing, the original audiogram forms were mailed via Canada Post to TransAlta’s office.
- By January 14, 2011, the audiogram forms had still not arrived in the mail. A TransAlta representative contacted the WSHS office manager on January 14, 2011 to inquire about the forms.
- WSHS confirmed in a letter that the forms had been sent at the end of November 2010 by Canada Post and therefore, the package could not be traced.
- On January 14, 2011, TransAlta made additional inquiries at its head office to determine if any packages were undeliverable. It also verified with the Sundance Administration building and warehouse to determine if the package had been

- 15 individuals were affected as a result of this incident.
- TransAlta provided a severed copy of an audiogram test result: the Employee Health Monitoring - Audiogram form. The personal information on the form for each of the 15 affected employees included:
 - Employee name;
 - Work location and occupation;
 - A unique employee number;
 - Date employed;
 - Home address;
 - Date of birth;
 - Age;
 - Home phone number;
 - Medical history (as it applies to an audiogram test) including:
 - Whether an employee currently has a cold or flu;
 - Whether they have or had: head injury, ear ache, ringing in ear, ear infection, sinus infection etc.;
 - Whether an employee has seen a doctor for hearing problems;
 - Whether an employee wears a hearing aid;
 - Whether an employee is exposed to recreational noise such as: loud music, snowmobiles, aircraft, farming etc.
 - Date of test and audiogram test result
- TransAlta stated that because the employees filled out the information on the audiometric forms, on many of the forms the employee's identification number had not been entered on the form. In any event, an employee's unique identification number is not sufficient to allow an individual to log on to the TransAlta intranet; a password and a logon id would also be required.
- TransAlta has not received any indication that the loss of the package has resulted in any disclosure of personal information, but has decided to notify the affected individuals in any event. TransAlta is currently in the process of notifying the affected employees about the loss of the audiometric test forms.
- As a result of this incident, TransAlta has confirmed with its service provider, WSHS that it will send employee personal information via courier in the future, so packages can be tracked.
- In addition, TransAlta has implemented a new process with all of its contractors who work with health related information to ensure that going forward, reports as sent in a way that can be tracked.

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

[10] Pursuant to section 5(2) of PIPA, TransAlta is responsible for WSHS' compliance with PIPA. Section 5(2) provides:

5(2) For the purposes of this Act, where an organization engages the service of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act.

[11] The audiometric forms containing the personal information of TransAlta employees did not arrive at TransAlta's offices after they had been mailed by WSHS. In my view, this constitutes a loss of personal information under PIPA.

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

[13] In order for me to require that TransAlta notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to those affected 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.

[14] TransAlta stated it had "not received any indication that the loss of the package ha[d] resulted in any disclosure of the personal information. Consequently, TransAlta's assessment of the risk of harm to individuals is low."

[15] In this case, the personal information at issue is of low to moderate sensitivity. Although some medical information was lost in the breach, it is not, in my view highly sensitive personal medical information. Much of the other personal information that was lost is of low sensitivity, such as: name, address and telephone number. The loss of the medical information and other personal information such as name, address and telephone number would likely not cause significant harm to individuals. However, these data elements combined with an individual's date of birth could be used to commit identity theft, which is a significant harm.

[16] In order for me to require TransAlta to notify its employees, however, there must also be a "real risk" of harm to the employees as a result of the incident. This standard does not require that 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.

[17] In deciding whether there exists a "real risk" of harm in this case, I considered that WSHS confirmed it had mailed the audiometric forms. As such, it appears the personal information was lost en route through Canada Post. Mail services, such as

Canada Post are often targeted for identity theft and other criminal activity. The fact that TransAlta has not yet received any indication that the lost personal information has been accessed or disclosed does not mean there is no real risk. The information is in the form of paper records which are readily accessible and can be used by anyone who may find the information. Consequently, the loss of the information presents a real risk of harm to the individuals.

V. Decision

[18] Based on the information reported to me by TransAlta, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require TransAlta to notify its affected employees in accordance with section 19.1 of the *Personal Information Protection Act Regulation*.

[19] I note that TransAlta states it is in the process of notifying the affected individuals. TransAlta should confirm in writing to my Office that it has notified the affected individuals on or before March 8, 2011.

Frank Work, Q.C.
Information and Privacy Commissioner