

ALBERTA
**OFFICE OF THE INFORMATION AND
PRIVACY COMMISSIONER**

P2011-ND-015

SUNCOR ENERGY INC.

May 16, 2011

(Case File #P1865)

I. Introduction

[1] On April 27, 2011 I received a report from Suncor Energy Inc. (Suncor) 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 Suncor 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 Suncor 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). The unauthorized disclosure of information originated at Suncor’s head office located in Calgary, Alberta, even though the affected individuals reside in the province of Quebec.

[6] In considering whether to require Suncor 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 April 27, 2011, I received a written report from Suncor describing an incident involving the unauthorized disclosure of personal information.

[8] On May 16, 2011, my Office contacted Suncor to request that it provide additional information concerning the incident, in order for me to determine whether to require Suncor to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a telephone call on the same date.

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

- Revised income tax reporting statements, T4 and Relevé (tax reporting statements for Quebec residents) were mailed from Suncor’s head office in Calgary to 116 employees of Suncor’s Montreal Refinery during the week of April 15-21, 2011.
- Suncor advised that the two statements were manually matched up and mailed in one envelope.
- The T4 and Relevé statements include the name of the employee, mailing address, social insurance number, income, and deductions.
- An employee on April 20, 2011, contacted Suncor and advised that they had received someone else’s tax statements.
- On April 27, 2011, Suncor emailed a notice to all affected employees informing them that in a small number of cases tax slips for one employee were inadvertently enclosed in an envelope addressed to another employee. The notice asked employees to immediately contact the Human Resource advisor if they had received a slip in error. The notice appeared in English and French.
- As of May 16, 2011, a total of three employees have reported they received tax statements in error. All three employees returned the tax statements to either the Human Resource Advisor or provided the statement to the correct employee directly.

- Suncor submitted that since the tax statements were required to file income taxes by the end of April, most employees would have discovered and reported the error by the time it submitted the breach report to my Office.
- Suncor also advised it revised the procedure for mailing out tax statements to require one tax statement per envelope. Windowed envelopes will be used to display the name and mailing address of the recipient.
- Suncor also advised it would seek statements from the individuals who received tax statements in error that they had not retained or would not use or disclose any information received in error.

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 Suncor 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 Suncor 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 Suncor notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to those individuals 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 high sensitivity as it includes the name of the employee, mailing address, social insurance number, income, and deductions.

[13] Suncor also noted that the type of harm that could result from the unauthorized access to or disclosure of this information is identity theft, which, in my view, is a significant harm. Suncor also submitted that the risk of this harm was low as the affected employees were part of the same co-worker group at one location and if any information was wrongfully used there was a high probability it would be discovered.

[14] In order for me to require Suncor to notify the affected individuals, however, there must also be a “real risk” of harm to the individuals 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.

[15] In deciding whether there exists a “real risk” of harm in this case, I considered that Suncor notified the affected groups of individuals soon after the incident was discovered, the information submitted by Suncor and the type of information involved.

[16] Despite Suncor’s submission that the work group involved is small and therefore the likelihood of the information being used wrongfully is low, given the sensitivity of the personal information of the employees, I have decided that there is a real risk of

significant harm to those individuals whose tax statements were mailed to individuals who were not authorized to receive the information.

V. Decision

[17] I understand that Suncor has notified the three affected individuals by way of its April 27, 2011, email to the employees of the Montreal Refinery who may have been by the error. However, s.37.1 (1)(a) of PIPA permits me to require that Suncor notify the three affected individuals whose tax statements were mailed to individuals who were not authorized to receive the information “in a form and manner prescribed by the regulations.” Therefore, I require Suncor to notify the three affected individuals, and any further affected individuals that may come forward, in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, if it has not already done so.

Frank Work, Q.C.
Information and Privacy Commissioner