

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

P2010-ND-004

RADCAN ENERGY SERVICES INC.

September 29, 2010

(Case File #P1666)

I. Introduction

[1] On September 9, 2010, I received a report from Radcan Energy Services Inc. (Radcan) 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 an individual as a result of the incident, and therefore I require that Radcan notify the individual to whom there is a real risk of significant harm.

II. Jurisdiction

[2] PIPA applies to provincially-regulated private sector organizations in Alberta. I have jurisdiction in this case because Radcan is an “organization”, as defined in section 1(i) of the Act, operating in the province of Alberta.

[3] 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.

[4] 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.

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

III. Background

[6] On September 9, 2010, I received a written report from Radcan describing an incident involving the unauthorized disclosure of personal information.

[7] On September 15, 2010, my Office contacted Radcan to request that it provide additional information concerning the incident, in order for me to determine whether to require that it notify individuals under subsection 37.1(1) of PIPA. My Office received Radcan's response on September 20, 2010.

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

- Late the afternoon of September 8, 2010, a manager emailed a work schedule to Radcan's President and copied it to six employees. However, the manager accidentally attached it to a previous string of email exchanges which contained a discussion regarding the potential termination of one of the employees copied on the email and which specifically named the employee.
- The error was discovered the next morning by an administrative assistant who opened and read the email. The administrative assistant immediately notified the HR manager.
- The HR manager then sent an e-mail to each of the five employees who had been copied on the email advising that the email had been sent accidentally and if they had opened the email it was not to be discussed with anyone and if they had not received the email to please disregard it and immediately delete it. The HR manager also sent an email to the sixth employee whose potential termination had been discussed, advising the employee that an email had been sent out the day before which disclosed the employee's name and information regarding the employee's employment with Radcan. The HR manager further advised in the email that Radcan had taken immediate action by talking to all employees who were cc'd on the email and had asked them to disregard and delete the email immediately, as it was sent out by mistake. The HR Manager further apologized for the lapse of judgment on Radcan's part and indicated the President would be contacting the employee shortly to discuss the mistake.
- Radcan advised that as a result of this incident, it would be reviewing its privacy policy with each employee and providing additional training to the manager who made the mistake of sending out the email, on the importance of privacy and the laws that relate to privacy.

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

[9] Pursuant to section 37.1 of PIPA, I have the power to require Radcan 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 Radcan to

notify its employee, I must consider whether there exists a “real risk of significant harm” to individuals as a result of the incident.

[10] In order for me to require that Radcan notify its employee, there must be some harm – some damage or detriment or injury – that could be caused to that employee as a result of the incident; moreover, that harm must be “significant” – it must be important, meaningful, and with non-trivial consequences or effects.

[11] The harm that can flow from the unauthorized disclosure of personal information can take many forms. For example, where SIN or credit card numbers are disclosed, this can lead to identity theft. Other disclosures of personal information can lead to the risk of physical harm to individuals. In the case at hand, the harm is the damage to the reputation of the employee whose possible termination was disclosed in the email.

[14] In order for me to require Radcan to notify its employee, however, there must also be a “real risk” of harm to the employee 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] I note that while Radcan acted quickly to contact the employees to whom the email was sent to instruct them to delete and disregard the email, at least one individual had already read the information.

[16] Given the sensitivity of the information, I believe there to be a real risk of significant harm in this case.

V. Decision

[17] Based on the information reported to me by Radcan, I have concluded there is a real risk of significant harm to the individual whose employment status was discussed in the email and I require Radcan to notify this individual.

[18] I understand Radcan has already notified the individual by way of the email sent on September 9, 2010.

Frank Work, Q.C.
Information and Privacy Commissioner