ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-07

Teamsters Local Union 987 of Alberta

January 18, 2013

(Case File #P2190)

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 November 9, 2012, Teamsters Local Union 987 of Alberta (the "Organization") provided notice of an incident involving the unauthorized 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 a trade union as defined in the *Labour Relations Code*. 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 following information of 12 employees (the "Affected Individuals"):

- first and last name,
- annual salary, and
- salary increase or bonus received each year for 2 years that was in addition to the annual salary increase.

[7] This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On November 29, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between November 29, 2012, and January 11, 2013.

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

- A former employee of the Organization is alleged to have distributed the personal information of the Affected Individuals to 20 fellow employees and others known to the Organization (the "Recipients").
- The personal information was contained in a document (the "Document"). The Document was left at the residence of each Recipient.
- The former employee had authorized access to the personal information when employed by the Organization.
- The Organization changed all passwords on the network after learning of the incident. It also confirmed that the former employee did not have access to the network following the end of the employment tenure.

- The Organization requested the Recipients to return or destroy the Document. Six Documents have been returned to the Organization. It has been unable to reach the Recipients who are not employees to request the Document be destroyed.
- The Organization notified all employees, including the Affected Individuals, about the incident in a letter dated November 8, 2012.

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 that this incident presented a risk of identity theft. It also reported that the bonus for each Affected Individual differed and the amount received was discretionary and linked to job duties or performance. As a result, it said the Affected Individuals could suffer a risk of hurt, humiliation and damage to relationships as a result of this incident.

[14] The personal information at issue is of low to moderate sensitivity, as it involves name, salary, and bonus information of the Affected Individuals. The harm that could occur to the Affected Individuals as a result of the unauthorized disclosure of the personal information, specifically the discretionary bonus, is hurt, humiliation and damage to relationships. In my view, these are significant harms.

[15] 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.

[16] The Organization reported that, although salary and wage increases are not generally known between employees, the work environment is not particularly sensitive to wage amounts.

[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 personal information at issue is of low to moderate sensitivity.
- A former employee with authorized access to the personal information during her employment allegedly disclosed the personal information without authorization.
- The disclosure was to current coworkers of the Affected Individuals.
- The bonus was discretionary and varied between the Affected Individuals depending on job duties or performance.
- Not all Recipients could be contacted to return or destroy the Document.

[18] In P2012-ND-06, I decided there was a real risk of significant harm to the affected individuals whose personal information, including name and income, was inadvertently disclosed to coworkers of an organization. Two important factors I used to determine whether there was a real risk of humiliation and damage to reputation to the affected individuals was that the incident involved commission salaries and the competitive nature of the business involved.

[19] In P2012-ND-10, the affected individuals and the unintended recipients of the sensitive personal information continued to work together or maintained some element of physical or work related proximity. These factors were important with respect to my determination that there was a real risk of significant harm with respect to hurt, humiliation and damage to reputation of the affected individuals in that case.

[20] The unauthorized disclosure in this case occurred primarily to current coworkers who have a continuing relationship with the Affected Individuals. The bonus was discretionary and varied in amounts between individuals. The discretionary bonuses were tied to performance or job duties, similar to the commission salaries in P2012-ND-06.

[21] 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

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

[23] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in a letter sent on November 8, 2012. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner