ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-26

ROBERTSON BRIGHT INC.

June 21, 2013

(Case File #P2272)

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 February 22, 2013, Robertson Bright Inc. (Organization) provided notice of an incident involving the unauthorized access to or 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 an extra-provincial corporation registered and operating in Alberta. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i)(i)of PIPA.

[6] The Organization reported the incident involved 36 Alberta employees with respect to the following information:

- name,
- address,
- social insurance number, and
- total earnings and deductions for 2012.

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

III. Background

[8] On April 15, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between April 18 and May 17, 2013.

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

- On February 15, 2013, an employee reported the T4 information of another employee had been printed on his or her T4 form.
- The Organization investigated and discovered that the T4 information for 36 employees was printed in error on the T4 forms of 36 fellow employees.
- The Organization notified the affected employees whose personal information was printed in error on another employee's T4 form about the incident in a letter on February 22, 2013.
- The same letter was also sent to the 36 employees who received another employee's T4 information in error and requested the return of the T4 information to the Organization.

- The Organization was also able to contact 19 employees by telephone who had received information in error. Seven employees returned the T4 information received in error and 12 confirmed they had destroyed it. All 19 confirmed either orally or in writing that they did not copy or would not use or disclose any information received in error.
- For the 17 employees who could not be reached by phone, the Organization also sent an email on May 1, 2013, requesting the return or destruction of the information.
- The Organization has not received a response from these 17 employees. These employees may have been temporary workers or the contact information is no longer valid.

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 employees, 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 employees, I must consider if there is a "real risk of significant harm" to the affected employees as a result of the incident.

[12] In order for me to require that the Organization notify the affected employees, 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. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[13] Due to the highly sensitive nature of the information, the Organization submitted the affected employees may experience identity theft or damage to reputation and humiliation as a result of this incident.

[14] In my view, the personal information at issue is highly sensitive. It includes the social insurance number of the affected employees. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft or fraud. The affected employees' total earnings were also disclosed to fellow employees. The Organization identified the harms of damage to reputation and humiliation for those affected employees. In my view, these are significant harms.

[15] In order for me to require the Organization to notify the affected employees, there must also be a "real risk" of significant harm to the affected 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. There must be a cause and effect relationship between the incident and the possible harm.

[16] The Organization reported the incident did not pose a "real risk" of significant harm for the following reasons:

- The employees who received the information in error are known to the Organization and fellow employees.
- The incident occurred as a result of an error and not malicious intent.
- The earnings of affected employees are not commission based and are standard for the industry.
- All but 4 affected employees are field workers who do not work in close proximity to other employees.

[17] The Organization, however, did recognize the real risk of significant harm may increase if the Organization is unable to secure the return or destruction of the T4 information released in error.

[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] With respect to this incident, I rely on the reasons provided by the Organization to support the decision that there is no real risk of significant harm with respect to harms of damage to reputation and humiliation. This workplace does not involve earnings tied to performance or competition. The majority of the affected employees do not work in close proximity to each other.

[20] However, based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm for identity theft or fraud to the 17 affected employees whose T4 information cannot be recovered or confirmed destroyed by the Organization as a result of this incident. While the Organization continues to make an effort to recover the information, the sensitive nature of the personal information and the fact that the Organization has been unable to confirm the destruction or retrieve the information for these affected employees contributed significantly to my decision.

V. Decision

[21] I require the Organization to notify the 17 affected employees whose personal information has not been returned to the Organization or confirmed destroyed in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

[22] I understand that the Organization notified these affected employees in accordance with the Regulation in a letter sent on February 22, 2013. Therefore, I will not require the Organization to notify these employees again.

Jill Clayton
Information and Privacy Commissioner