ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-08

CHIVERS CARPENTER LAWYERS

July 23, 2012

(Case File #P 2070)

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 27, 2012, Chivers Carpenter Lawyers (the "Organization") provided notice of an incident involving the loss 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 partnership as defined in the *Partnership Act.* 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 contained in 2 briefcases:

- In the first briefcase (Briefcase 1) information of the Organization's client contained in file folders:
    - general correspondence with the administrative tribunal and opposing counsel
    - first and last names of 30 individuals with some or all of the following information: home address, home or cell phone number, email address; name of current or previous employer;
    - a record of employment for one of the 30 individuals containing his or her first and last name, address, and social insurance number; and
    - a performance evaluation containing general feedback about performance which was positive in nature for one of the 30 individuals may also have been in Briefcase 1.

- In the second briefcase (Briefcase 2) information contained in 3 binders:
    - Binder 1: copies of general correspondence contained in Briefcase 1; and
    - Binder 2: personnel files for 6 individuals containing the following information:
        - records of employment containing first and last name, home address, and social insurance number;
        - tax credit forms containing first and last name, home address, and social insurance number;
        - health benefit forms containing first and last name, home address, home phone number, date of birth, marital status, social insurance number, and name of beneficiary;

        - employment resumes containing first and last name, contact information, employment history;
        - banking information for direct deposit containing account number or void cheque;
        - performance evaluations;
        - payroll information containing first and last name, home address and phone number, birth date, social insurance number, expense forms, sick sheets, and training received;
    - Binder 3: lawyers notes about the 6 individuals' work experience
        - contact information for the 6 individuals.

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

III. Background

[8] On March 5, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between March 5, and July 11, 2012 in a number of telephone calls and emails.

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

- On February 20, 2012, a lawyer who was an employee of the Organization had her vehicle broken into. In her vehicle were Briefcase 1 and Briefcase 2. Briefcase 1 was stolen from the vehicle. It was not recovered.
- Briefcase 2 was not stolen. The lawyer reported that:
    - Briefcase 2 appeared to be intact with no items disturbed or removed;
    - Briefcase 2 was in the same spot in the car where it was left, which was wedged on the floor in the back seat; and
    - The employee believes that the perpetrator did not view the contents of Briefcase 2.
- The Organization reported the theft to the Edmonton Police Service.
- The Organization confirmed there are 30 individuals affected by the loss of personal information from Briefcase 1.
- The Organization notified these 30 individuals by letter on February 24, 2012.
- The Organization did not notify the 6 individuals whose personal information was contained in Briefcase 2.

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 there is no real risk of significant harm that could occur to the 30 individuals as a result of the theft of their first and last name, home address, home and cell phone number, email address, and name of current or previous employer. The reason provided is that this information is mostly publicly available and of low sensitivity. The Organization also indicated that no real risk of significant harm could occur to the individual whose performance evaluation may have been contained in Briefcase 1. The reason provided is that this information is not highly sensitive. The Organization stated, however, that there is a risk of significant harm, identity theft, to the one affected individual whose record of employment was stolen. This is because the social insurance number contained in the record is highly sensitive. The Organization did not provide an analysis of real risk of significant harm for Briefcase 2.

[14] With respect to Briefcase 1, I agree with the Organization that the personal information of the 30 individuals is of low sensitivity and that there is no risk of significant harm that could occur to these individuals as a result of this incident. I also agree that the performance evaluation information for the one individual is of low sensitivity and that there is no risk of significant harm that could occur as a result of this incident to this individual. For these individuals, the first part of the test of requiring notification – that the incident could result in significant harm to these individuals – is not met. Given this, I do not need to decide whether there is any "real risk" of significant harm to these individuals. However, for the one individual whose record of employment was stolen, the social insurance number is highly sensitive and the harm that could occur to this individual is identity theft or fraud. In my view, this is a significant harm.

[15] With respect to Briefcase 2, my findings regarding the copies of the personal information contained in Briefcase 1 is the same. For the 6 individuals whose personnel records were in Briefcase 2, this information is highly sensitive and could be used to commit identity theft or fraud. In my view this is a significant harm.

[16 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.

[17] With respect to Briefcase 1, in deciding whether there exists a "real risk" of significant harm in this case to the one affected individual whose record of employment containing his or her social insurance number was stolen, I considered the following factors:

- The personal information is highly sensitive.
- The information was stolen out of a vehicle indicating a loss that resulted from a theft by someone with nefarious intentions.
- The personal information at issue has not been recovered.

In breach notification decision P2012-ND-01, I determined that highly sensitive information stolen out of a vehicle and viewed by individual(s) not authorized to have access to the personal information were factors in determining a real risk of significant harm to the individuals in that case.

[18] Based on the information reported to me by the Organization, I have decided that there is a real risk of significant harm to the one individual whose record of employment was stolen as a result of this incident.

[19] With respect to Briefcase 2, based on the report by the Organization it does not appear that the thief removed any of the contents, nor even accessed the briefcase. In my view, had the thief accessed the briefcase and intended to cause harm, it is likely Briefcase 2 would have been taken along with Briefcase 1. As this did not occur, I find there is no "real risk" of significant harm to these 6 individuals.

V. Decision

[20] I understand that the Organization has notified the individual whose record of employment was stolen in accordance with the Regulation in a letter sent on April 24, 2012. Therefore, I will not require the Organization to notify this individual again.

Jill Clayton
Information and Privacy Commissioner