ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-039

ZELLERS DRUG STORES (ALTA) LIMITED

November 30, 2011

(Case File #P2031)

I. Introduction

[1] On November 22, 2011, I received a report from Zellers Drug Stores (Alta) Limited ("Zellers Pharmacy" or the "Organization") of an incident involving the loss of and unauthorized access to 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 Zellers Pharmacy 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 Zeller Pharmacy 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).

[6] In considering whether to require Zellers Pharmacy 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 November 22, 2011, I received a written report from Zellers Pharmacy describing an incident involving the loss of and unauthorized access to personal information as a result of a theft.

[8] On November 23, 2011, my Office contacted Zellers Pharmacy to request that it provide additional information concerning the incident, in order for me to determine whether to require Zellers Pharmacy to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and e-mail correspondence between November 23 and November 25, 2011.

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

- In the early morning of November 21, 2011, it was discovered that a locked safe within a Zellers Pharmacy in Edmonton, Alberta was stolen.
- The safe contained, among other things, narcotics and a notebook with personal information of nine Zellers Pharmacy customers.
- The personal information stolen includes:
    - Name;
    - Credit card number;
    - Credit card expiry date.
- There was no treatment or care information of the nine affected individuals. The safe was used to store narcotics, and it is believed that the narcotics were the target of the thieves. The personal information contained in the notebook for the

nine customers was in the safe because those were regular customers who were unable to attend the Zellers Pharmacy in person to fill their prescriptions. Zellers Pharmacy is PCI compliant which means that no credit card numbers are stored on the pharmacy system. As such, those nine customers with special needs who could not fill their prescriptions in person had their personal information written down and stored in the safe.

- Zellers Pharmacy reports that law enforcement authorities immediately responded to the alarm triggered by the theft. Surveillance video of the theft is being reviewed in an attempt to identify the perpetrators.
- In accordance with PCI requirements, Zellers Pharmacy is in the process of alerting the credit card companies of the theft.
- The nine affected individuals were notified of the incident on November 23, 2011 in a letter hand delivered by messenger.

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 Zellers Pharmacy 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 Zellers Pharmacy 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 Zellers Pharmacy notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the nine customers 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 customer name, credit card numbers, and credit card expiry dates. This is information that could be used to commit identity theft. In addition, the personal information was stolen by thieves who were, most likely, after the narcotics kept in a safe. It can be assumed that the perpetrators had the intent of stealing the narcotics and subsequently selling them for a profit. If monetary gain was the motive, access to the credit card information would be of benefit to those individuals.

[13] Zellers Pharmacy also noted that the type of harm that could result from the unauthorized access to this information is identity theft, which, in my view, is a significant harm. Zellers Pharmacy acknowledged that given the nature of the personal information at issue, and the manner in which it was breached that there is a "real risk of substantial harm". Moreover, the thieves could apply false charges to the credit cards and potentially open new and false credit facilities using the information stolen, or could perpetrate identity theft.

[14] In order for me to require Zellers Pharmacy to notify the affected customers however, there must also be a "real risk" of significant harm to the customers 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. 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 the personal information was stolen by thieves who clearly had nefarious intentions, and that the personal information is of high sensitivity and could be used to commit identity theft in the form of fraud.

[16] Given the information reported by Zellers Pharmacy, I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the following factors: the type of information involved could be used to commit identity theft, which is a significant harm; and the personal information at issue was stolen.

V. Decision

[17] Based on the information reported to me by Zellers Pharmacy, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Zellers Pharmacy to notify affected individuals. I understand Zellers Pharmacy has already notified the individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of letter hand delivered by courier on November 23, 2011; therefore I will not require Zellers Pharmacy to notify again. I commend Zellers Pharmacy for notifying this Office, and subsequently the affected individuals, without delay.

Frank Work, Q.C.
Information and Privacy Commissioner