ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-02

Costco Wholesale Canada Ltd.

February 13, 2013

(Case File #P2229)

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 December 19, 2012, Costco Wholesale Ltd. (the "Organization") provided notice of an incident involving the unauthorized access to 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 federal corporation extra-provincially registered and operating in Alberta. 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:

- credit card number,
- debit card number, and
- the personal identification number ("PIN") associated with the cards may have been compromised as well.

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

III. Background

[8] On January 4, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization on January 7, 2013.

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

- On December 7, 2012, American Express notified the Organization that card skimming activity occurred at 1 or more of the Organization's locations in Calgary, Okotoks, and Rocky View. Further, American Express advised the Organization that approximately 22 credit cards were duplicated and used in a fraudulent manner as a result of the skimming that occurred.
- As part of the Organization's internal investigation, video surveillance tapes were reviewed and the Organization confirmed that skimming devices were installed on 4 gas pumps in Calgary, Okotoks, and Rocky View between November 12, 2012, and November 16, 2012. Since the skimming devices were installed and then removed within the same day, the Organization cannot confirm whether the skimming devices captured the PIN as well.

- A total of 529 customers (the "Affected Individuals") were affected by the incident.
- The Organization reported the incident to the Calgary Police Service and the RCMP detachments in Okotoks and Rocky View.
- As a result of the incident, the Organization altered its security practices in order to prevent skimming.
- The Affected Individuals were notified by telephone and mail on December 14, 2012, and December 18, 2012.
- The Organization notified its debit card and credit card processor of the skimming event.

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 the incident posed a significant risk of identity theft and fraud to the Affected Individuals given that some credit and debit card numbers were duplicated and used in a fraudulent manner.

[14] In my view, the personal information at issue is highly sensitive. It includes credit and debit card numbers of the Affected Individuals. The type of harm that could result from unauthorized access to this personal information is identity theft or fraud. If PIN numbers were accessed during the skimming, the Affected Individuals could also suffer financial losses. 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] In deciding whether there exists a "real risk" of significant harm in this incident to the Affected Individuals, I considered the following factors:

- The personal information is highly sensitive. It could be used to commit identity theft and fraud, and result in financial losses to the Affected Individuals.
- The personal information was skimmed and used for fraudulent purposes.

[17] In P2011-ND-001 and P2012-ND-27 highly sensitive personal information was skimmed and used for fraudulent purposes. In these cases, it was decided that there was a real risk of significant harm to the affected individuals.

[18] 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

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

[20] I understand that the Organization notified the Affected Individuals in accordance with the Regulation by telephone and mail on December 14, 2012, and December 18, 2012. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner