ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-18

SCULPZ, INC. operating as ENCHANTRESS HOSIERY OF CANADA

May 9, 2013

(Case File #P2301)

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 April 2, 2013, Sculptz, Inc. operating as Enchantress Hosiery of Canada (Organization) provided notice of an incident involving the unauthorized access to and 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 incorporated in Delaware, in the United States of America (USA). The incident involved a website located on a server located in the USA. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA and the incident involves personal information provided to the Organization by Alberta residents through the Organization's website.

[6] The Organization reported the incident involved the following customer information:

- name,
- address,
- phone number,
- email address,
- credit card number and expiry date.

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

III. Background

[8] On April 10, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization On April 10, 2013.

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

- On March 11, 2013, the Organization discovered during a scheduled security review that the Organization's website had been hacked.
- The website server log showed access by an unauthorized individual(s) on March 5, and 9, 2013, to the personal information at issue.
- The credit card information was not encrypted.
- The total number of customers affected is 814. This included 154 Alberta customers (Affected Individuals).

- The website was taken offline on March 11, 2013. The website will not be brought back online until the vulnerability is corrected and the customer information encrypted.
- The Organization notified Affected Individuals by mail on March 20, 2013, regarding the incident.

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 the incident did pose a risk of significant harm. The Organization recognized the unencrypted credit card information could be used to fraudulently purchase products from other online merchants who do not require a CVV2 security code. The credit card information could also be sold.

[14] In my view, the personal information at issue is highly sensitive. It includes the credit card information and email addresses of a significant number of individuals. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft or fraud. Since a significant number of email addresses, addresses and phone numbers were involved, the Affected Individuals may also be at risk for phishing. 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 the incident involved criminal intent. The Organization submits the hacker was after the credit card information. However, whether

or not the hacker would be successful in making fraudulent purchases with the credit card information would depend on whether online merchants would accept the credit card information without a CVV2 or security code.

[17] In P2012-ND-25 and P2012-ND-02, the personal information involved combined with the fact the incident involved hacking contributed to my decision that the affected individuals were at a real risk of significant harm for identity theft and fraud. I also recognized in those decisions that access to a significant number email addresses increased the risk of phishing.

[18] In P2012-ND-27, a hack of a wireless network resulted in unauthorized access to credit card number and expiry date information without the associated CVV2 or security code. I decided in that case that the incident posed a real risk of significant harm for fraud and identity theft with respect to the name, credit card number and expiry date of affected individuals.

[19] 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. This incident involved hacking. The Organization confirmed the website was accessed on two occasions by the hacker(s). The personal information included access to plain text credit card information and expiry date, in addition to other personal information such as email addresses and contact information. In my view, these factors indicate there is a real risk of significant harm to the Affected Individuals as a result of this incident.

V. Decision

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

[21] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in a letter sent on March 20, 2013. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner