ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-14

Crafts Americana Group, Inc.

May 6, 2013

(Case File #P2251)

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 11, 2013, Crafts Americana Group, Inc. (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 located in Vancouver, Washington, U.S.A. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA and the personal information was collected from Alberta residents through the Organization's websites.

[6] The Organization reported the incident involved the following information of its customers:

- name,
- address,
- phone number,
- credit card number, expiration date, and security code.

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

III. Background

[8] On April 17, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization April 23, 2013.

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

- On January 25, 2013, a payment processor notified the Organization about a number of unauthorized transactions involving Organization customers.
- The Organization investigated and discovered an unauthorized file on one of its servers.
- The file contained the personal information of customers who had purchased merchandise through 3 of the Organization's websites.
- Credit card numbers in the file were matched to unauthorized transactions reported to the Organization.

- The Organization determined that an unauthorized individual(s) exploited a software vulnerability to access the server and create the file.
- The total number of customers affected in the U.S.A. and Canada is 12,300. This includes 139 customers from Alberta (Affected Individuals).
- The Organization removed the file and notified the appropriate law enforcement authority.
- The vulnerability was patched. Security measures were applied to prevent similar incidents.
- Credit card information is no longer retained.
- Customers were notified of the incident by mail on February 8, 2013, or, in the case of customers with Canadian addresses, February 20, 2013.

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 not pose a further risk of significant harm because it had notified card issuers and the payment processor of the incident. Further fraudulent transactions would, therefore, be unlikely. New credit card numbers would likely be issued to the customers.

[14] The personal information is highly sensitive. The type of harm that could, and did, result from unauthorized access to and disclosure of the personal information is identity theft and fraud. 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] 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. The highly sensitive personal information involved in this incident was accessed by an unauthorized individual(s). This personal information was used for fraudulent transactions.

V. Decision

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

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

Jill Clayton
Information and Privacy Commissioner