ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-09

THE BRICK WAREHOUSE LP

May 15, 2012

(Case File #P2032)

I. Introduction

[1] On November 24, 2011, I received a report from The Brick Warehouse LP ("The Brick" or the "Organization") of an incident involving the 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 The Brick 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 The Brick 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 The Brick 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 24, 2011, I received a written report from The Brick describing an incident involving the unauthorized access to personal information of the Organization's customers who had signed up for an online contest.

[8] On November 25, 2011, my Office contacted The Brick to request that it provide additional information concerning the incident, in order for me to determine whether to require The Brick to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls, faxes, and emails between November 25, 2011 and March 6, 2012.

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

- The Brick held an online contest across Canada called "The Brick Prize Couch Flip it to Win Promotion". The contest ran between October 11 and November 3, 2011. Contestants provided the following personal information in order to be eligible to win a prize as part of the contest:
    - First and last name;
    - Email address; and,
    - Language preference (English or French).

- The personal information was stored in a database hosted by a third party service provider contracted by The Brick to forward coupons associated with the contest.

- On November 17, 2011, employees at The Brick who had set up email accounts for the purposes of testing the contest website received spam email that The Brick believes was sent by an organization, 'PT' based on the spam received. In addition, The Brick reported that it received comments on its Facebook page from contestants who had also received the spam email. It is not known whether all 29,300 individuals who signed up for the contest received the spam email, but The Brick has assumed they all did. The number of affected individuals in Alberta is not known as the contestants did not provide a province of residence.

- The Brick has investigated the incident, but reported that it was unable to determine how the database was accessed. The Brick reported that its investigation into the incident did not determine any connection between the third party service provider hosting the database and PT or between PT and The Brick. The spam email purportedly sent by PT includes a link stating PT designed the contest website; The Brick has confirmed that this is false. The Brick further reports that its attempts to ascertain PT's involvement in the breach have been met with silence.

- Following its discovery of the unauthorized access, The Brick changed the passwords to the database and had the database transferred from the third party service provider's possession back to The Brick's possession. The third party service provider confirmed in writing that its internal and third party email environments were not breached.

- On November 18, 2011, The Brick sent an email notification to all 29,300 affected individuals advising them of the incident. Included among those individuals were people who may have opted out from receiving coupons.

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 The Brick to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure" of personal information. In determining whether or not to require The Brick 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 The Brick notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the contestants 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] The Brick noted that there was a low risk that harm could result from the unauthorized access to this information. The Organization did not believe the

information could be used to commit fraud unless an online contestant provided additional information in response to the spam email.

[13] The personal information at issue is of low sensitivity as it includes name, email address, and language preference. However, the large number of email addresses that may have been acquired by PT suggests that the type of harm that could occur to the affected individuals is phishing. Phishing attempts may target individuals as customers of the Brick to encourage them to open malware attachments or click on links which will prompt them to provide additional personal information.

[14] In order for me to require The Brick to notify the contestants, however, there must also be a "real risk" of significant harm to the 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. 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 significant harm in this case, I considered that contestants received the spam email after they entered the contest, that the cause of the breach is unknown and a large amount of email addresses were involved in the breach. These circumstances taken together create the likelihood that The Brick contestants' personal information will be used in the future for the purposes of phishing, which is a significant harm. Similar circumstances can be found in case P2011-ND-018. While there is a general awareness among internet users to recognize and not respond to phishing attempts, given the magnitude of this breach (i.e. the number of affected individuals), I find that there is a real risk of significant harm in this matter.

[16] While The Brick does not believe the possibility of phishing is likely, they state that it is possible. At this point it is unknown if additional emails have been sent to The Brick contestants that went beyond spam and turned into phishing attempts, or if any will be sent in the future as a result of the unauthorized access.

[17] Given the information reported by The Brick, 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: although the type of personal information accessed is of low sensitivity, the cause of the breach is unknown, plus a large number of email addresses were involved in the breach and used to spam the affected individuals creating the likelihood that the affected individuals will suffer the harm of phishing.

V. Decision

[18] Based on the information reported to me by The Brick, I have concluded that there is a real risk of significant harm to individuals as a result of this incident. The Brick has already provided notification to the affected individuals; however, the notification is not compliant with section 19.1(b)(iv) of the *Personal Information Protection Act Regulation*. Therefore, the Brick will be required to re-notify the affected individuals and

provide additional details on the steps it has taken to reduce the risk of harm. I require the Brick to confirm to me that it has done so on or before June 4, 2012.

Jill Clayton
Information and Privacy Commissioner