ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-15

BILLABONG INTERNATIONAL LIMITED

July 18, 2013

(Case File #P2192)

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 November 15, 2012, Billabong International Limited (the Organization) provided notice of two incidents 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 headquartered in Queensland, Australia. The information at issue was in databases stored on a server hosted by an external service provider located in California, 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 collected from Alberta residents.

[6] The Organization reported the incidents involved all or some combination of the following information stored in its databases:

- name,
- address,
- telephone number and fax number (if provided),
- date of birth and age,
- gender,
- email addresses,
- IP addresses,
- blog comments, and
- hashed and plain text passwords.

[7] Where this information, or combinations thereof, is about identifiable individuals, it qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] Between December 19, 2012, and March 1, 2013, my Office requested the Organization provide additional information concerning the incidents. The additional information was provided by the Organization between January 9, 2013, and March 7, 2013.

[9] The Organization reported the circumstances of the incidents as follows:

- On October 23, 2012, the Organization learned an online technology blog was reporting that a hacking group claimed to have attacked one of the Organization's databases. The blog post reproduced Twitter posts made by the hacking group.

The Twitter posts stated that the Organization's databases had been "attacked & hacked" and included a hyperlink to a website where users post computer-related code. A post by the hacking group on this website claimed to have accessed an Organization database and included administrator account user IDs and hashed passwords associated with one of the Organization's websites. It stated that "more than 37,000 users are at risk due to this attack."

- On October 26, 2012, the Organization became aware of a Twitter post by another hacking group claiming to have attacked and hacked an Organization blog website. The Twitter post included a hyperlink to the same computer coding website as referenced above. A post by the hacking group on the website included administrator user IDs and plain text passwords for a number of blogs on an Organization website.
- Both postings on the computer coding website were removed on October 27, 2012.
- The Organization investigated the incidents. Audit log files showed unauthorized access to an Organization server hosted by an external service provider and located in California, USA, on October 23, 24 and 25, 2012. The Organization has no record of unauthorized access prior to these dates as the log files only contained three days' worth of data. It does not have an audit record with respect to access to the databases before those dates other than the fact the information posted by the hackers in the first attack came from tables on the server.
- There were 87 databases on the affected server, including those referred to on the computer coding website. A search of these databases identified 82 associated tables containing personal information. Three of the tables contained plain text passwords.
- No financial information (such as credit card details or bank account information) was stored on the affected server.
- The Organization identified 123 of the affected individuals as residents of Alberta. Of these, 121 had an email address involved in the incident. One individual's information included a plain text password.
- Following the incidents, the Organization:
    - secured the database,
    - removed the postings from the computer coding website,
    - removed affected files,
    - took steps to move the information from the service-provider hosted server to an Organization server,
    - reset passwords,
    - added security measures, and
    - continues to monitor websites for additional information posts.
- On November 6, 2012, the Organization sent an email notification of the incident to those individuals whose information involved a plain text password.

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 incidents did not involve sensitive information, such as financial information, social insurance numbers or drivers' licence numbers (no financial information was stored on the affected server). The personal information and the passwords involved were not connected to the Organization's separate e-commerce website. Most of the passwords in the databases were hashed. The Organization did recognize that personal information involved in the incident, in combination with a plain text password, could put individuals at risk for identity theft or fraud.

[14] In my view, the personal information at issue is of low to moderate sensitivity. It involves name, location and contact information, date of birth, gender, email address, and hashed and plain text passwords. This information could be used to cause harm in the form of identity theft, fraud, and 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 recognized that where plain text passwords were involved, there may be an increased risk of harm if the affected individuals used their email address and passwords on other websites. As a result, the Organization notified these individuals about the incidents. However, the Organization was of the view there was no real risk of significant harm to most affected individuals since financial or other sensitive data was not involved. Further, the Organization reported that, for the following reasons, the databases themselves may not have been accessed by the hackers:

- The log files show unauthorized access to the server that hosted the databases; however, there are no audit logs to show whether or not the databases themselves were compromised.
- There is a discrepancy between the number of users one hacking group claimed were affected and the number identified by the Organization.
- The Organization's IT team confirmed the user IDs and hashed passwords published by the hackers could not have been used to access other websites or the databases.
- No further information from the databases has been posted to the best of the Organization's knowledge.

[17] In P2012-ND-30, which involved this same Organization and the same server, I recognized that unauthorized access to a significant number of email addresses in combination with other personal information increases the risk of phishing.

[18] 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.

[19] After considering the above factors and information received from the Organization, 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 a deliberate hack, perpetrated by unauthorized individuals with nefarious intent. The audit logs available confirm access to the server between October 23, 24, and 25, 2012. The Organization does not have an audit log prior to October 23, 2012, however, the information posted online as a result of the first attack came from tables on the server. There are no audit logs to confirm or deny if the databases were accessed. The Organization notified individuals with plain text passwords and email addresses. However, there are a significant number of affected individuals with email addresses without a plain text password or with a hashed password that are, in my view, at risk for phishing. In my view, these factors, together with the nature of the personal information involved and the significant number of individuals affected, 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 Alberta accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation"). If the email notification sent by the Organization on November 6, 2012, included the one affected individual whose exposed information included a plain text password, I will not require the Organization to notify this affected individual again.

[21] The Organization is required to notify me in writing that it has notified the affected individuals on or before June 30, 2013.

Jill Clayton
Information and Privacy Commissioner