ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-30

BILLABONG INTERNATIONAL LIMITED

November 20, 2012

(Case File #P2160)

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 August 30, 2012, Billabong International Limited (the "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's headquarters is located in Queensland, Australia. The incident involved a hack into a database file (the "Database File") on servers located in California, USA. The incident involved information collected on the Organization's website from Alberta residents. 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 approximately 478 Alberta residents with respect to the following information contained the Database File:

- name,
- email address,
- home address (including state and country code),
- age,
- gender,
- password for the Organization website, and
- telephone number.

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

III. Background

[8] On October 1, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization October 5, 2012.

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

- The Organization was notified on July 13, 2012, that the Organization's website had been hacked by an unauthorized individual. The hack occurred on July 11, 2012.
- The Database File contained information collected between 2006 and August 2011. It was not linked to other Organization systems or databases.

- The Organization was informed the hacker posted approximately half of the data entries from the Database File on a website that provides computer programmers with a platform to post and share code.
- The Database File included 35, 000 unique email addresses. Through an analysis of country, state, and postal code information, the Organization identified approximately 478 Alberta residents (the "Affected Individuals") as being affected by the incident.
- The personal information was entered by Affected Individuals on the Organization website by individuals who wanted to receive information or promotional material.
- The data fields were in plain text format and not encrypted.
- Not all data fields were populated. The Organization supplied the following information concerning what percentage of data fields were not populated:
    - 26% did not contain passwords,
    - 71% did not include full addresses,
    - 70% did not include full name,
    - 86% did not contain a telephone number.
- The Organization took steps to reset email addresses and passwords that were also used in their online stores.
- The Database File was removed from the server on July 13, 2012.
- The Organization requested the internet service provider and the registrant of the website domain name remove the personal information posted on the website by the hacker. This information was removed from the website on July 18, 2012.
- Law enforcement agencies and data protection regulators were informed by the Organization.
- The Organization has committed to audit its IT systems, adopt a new information policy, and to review and audit its privacy compliance measures.
- The Organization now encrypts all personal information submitted on it's website as standard procedure.
- The Organization sent an email notification to all email addresses in the Database File with respect to the incident on July 17, 2012. The email notification encouraged the recipients to change their passwords on other websites if they used the same password and email used on the Organization's website.

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 personal information at issue is of low to moderate sensitivity. Not all of the data fields were populated. The name, address and phone number fields were not populated in a majority of the total number of individuals affected by the incident.

[14] The Organizations submission states that 35, 000 unique email addresses were involved in the incident. Over 75% of those addresses also had a password associated with it.

[15] Previous decisions have recognized that the type of harm that could result from unauthorized access to a large volume of email addresses is phishing. In combination with other personal information involved in this incident, especially when a password is involved with an email address, I have recognized that identity theft could also occur. I recognized in Breach Decision P2012-ND-04 that it is possible that individuals use the same password and email address to access other accounts. In my view, these are significant harms.

[16] 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.

[17] The Organization recognized the incident posed the possible risk that some individuals might use their email addresses and passwords to access the Organization's ecommerce website or other forums. The Organization, however, assessed the real risk of significant harm with respect to this incident as low for identity theft because it had acted swiftly to notify individuals and the compromised passwords served no functional purpose on the Organization's database. In addition, the Organization emphasized to individuals the importance of changing passwords in the email notification it sent with respect to the incident.

[18] In deciding whether there exists a "real risk" of significant harm in this case to the Affected Individuals, I considered the following factors:

- The personal information is of low to moderate sensitivity.
- Many of the personal information data fields were not populated.

- Due to the volume of passwords and email addresses involved, in combination with the other personal information fields, the incident poses a risk for phishing and identity theft.
- There were 35, 000 unique email addresses involved in the incident in addition to a substantial number of passwords to the Organization's website.
- The personal information was in plain text and not obscured or encrypted.
- The incident was the result of a hack.
- The personal information of half of the Database File fields was posted by the hacker on a website until it was removed on July 18, 2012.

[19] In previous decisions, the magnitude of the incident has been a factor when assessing real risk of significant harm with respect to unauthorized access or theft of a large volume of email addresses and passwords. While the total number of individuals affected by the incident, including the Affected Individuals in Alberta, is not as significant when compared with other incidents, for example in Breach Decisions P2011-ND-011 or P21012-ND-04, this incident distinguishes itself with respect to assessing real risk of significant harm due to the two following factors:

- The personal information involved was in plain text and email addresses appeared with almost 75% of passwords.
- The hacker published half the information in the Database File on a website, further exposing the plain text information to an unknown number of unauthorized individuals.

[20] 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

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

[22] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in an email sent on July 17, 2012. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner