ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-31

eHarmony

November 23, 2012

(Case File #P2173)

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 October 2, 2012, eHarmony (the "Organization") provided notice of an incident involving the unauthorized 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 the state of Delaware, in the U.S. The incident involved Alberta customers who provided information on the Organization's website. 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 the following information:

- name (first and possibly last name, if provided),
- email address,
- password,
- phone number (if provided),
- internally assigned user number,
- membership dates.

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

III. Background

[8] On October 2, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization on October 13, 2012, November 13, 2012, and November 22, 2012.

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

- On September 5, 2012, the Organization was notified by U.S. federal law enforcement that a breach ("the Incident") was discovered in connection with an undercover operation they were conducting.
- The Organization determined that records of 529,411 users were hacked. Of those records, 5,245 records belonged to Alberta residents (the "Affected Individuals").
- The hack occurred as a result of an unknown software program, which extracted the personal information between May and June, 2010.
- The passwords were encrypted.
- There were no reports of suspicious account activity by the Affected Individuals.
- The Organization revised its password encryption process and password policies as a preventative measure to reduce any chance of unauthorized access to the accounts.
- The Organization also hired a Network Security Engineer to increase the security of the Organization's network and its data.
- Upon notification of this breach, the Organization immediately reset all Affected Individuals' passwords.

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.

[12] 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.

[13] 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.

[14] Although the Organization did not report it, the fact that the Affected Individuals are members of the Organization is also their personal information, which forms a part of the information accessed by the hacker. I will consider this personal information as part of the personal information involved in this incident.

[15] The personal information at issue in this incident is of low to moderate sensitivity. Some of the Affected Individuals may have provided their full names and phone numbers. Email addresses were also provided. The harm that could occur to the Affected Individuals as a result of a breach of this information in this case is phishing. For the Affected Individuals who provided their full name and phone number, because they are members of the Organization they could also suffer damage to reputation, hurt or humiliation given the nature of the Organization's services. In my view, these are significant harms. Given that the passwords were encrypted, there is no risk of significant harm that could occur to the Affected Individuals as a result of a breach of this information.

[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 reported the incident did not pose a significant risk of harm to the Affected Individuals because all accounts were protected by an encrypted password. Further, upon discovery of the breach, the Organization erred on the side of caution and reset all Affected Individual's passwords and further enhanced their security protocols to protect the personal information in their databases and on their website.

[18] With respect to those Affected Individuals who are at risk to suffer damage to reputation, humiliation or hurt as a result of a breach of the personal information, in prior decisions involving this type of harm I considered proximity as an important factor in determining whether a real risk of significant harm exists to an individual. In this case, I do

not have enough evidence to determine if there is proximity between the Affected Individuals. Therefore, I am unable to determine in this case if there is a real risk that this significant harm, damage to reputation, humiliation or hurt, could occur.

[19] With respect to the significant harm of phishing, in deciding whether there exists a "real risk" that this significant harm will occur to the Affected Individuals in this case, I considered the following factors:

- The personal information disclosed is of low sensitivity.
- The information was accessed by a hacker with malicious intent.
- There is a large number of Affected Individuals involved in the Incident.

[20] In cases P2011-ND-011, P2011-ND-012, P2011-ND-021, and P2012-ND-09, which involved a breach of a similar type of personal information, a large number of email addresses were accessed by hacker. In these cases, it was decided that phishing posed a real risk of significant harm to the individuals involved in these cases.

[21] 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

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

[23] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in an email sent on October 2, 2012. Therefore, I will not require the Organization to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner