ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-11

Blizzard Entertainment Inc.

September 18, 2013

(Case File #P2224)

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 December 14, 2012, Blizzard Entertainment Inc. (the "Organization") notified me of an incident involving 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 a corporation based in Irvine, California, 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 involved in this incident was collected from Alberta residents.

[6] The information involved in the incident included:

- email addresses,
- answers to personal security questions,
- passwords, and
- phone numbers.

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

III. Background

[8] Between December 18, 2012, and January 25, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between January 9 and March 15, 2013.

[9] The Organization operates a gaming website. In order to play the games offered on the website, individuals are required to provide information. On August 4, 2012, the Organization determined that an external person(s) gained unauthorized access to its internal network servers. These servers contained four tables containing the personal information of the Organization's North American players. The Organization reported that the information in each table can be linked through customer identification numbers.

[10] The Organization confirmed approximately 246,000 players from Alberta were affected by the incident. The Organization is unable to confirm if any of the affected individuals are under the age of 18. The age of individuals is not collected by the Organization.

[11] Upon learning of the incident, the Organization notified law enforcement. It posted a notice on its website advising players to change their passwords and security answers, update their software, monitor their accounts and be aware of phishing attempts.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[12] 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.

[13] 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.

[14] 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.

[15] The Organization reported that there is a low probability the affected individuals would suffer harm because the passwords were cryptographically scrambled and financial information was not accessed.

[16] In my view, the personal information involved in the incident is of low to moderate sensitivity. There is no risk of significant harm to the affected individuals as a result of unauthorized access to the cryptographically scrambled versions of passwords or to the phone numbers, which were reported to be hashed. There is, however, a risk that phishing will occur due to the large number of email addresses involved in the incident. In my view, this is a significant harm.

[17] In order for me to require the Organization to notify the affected individuals, there must also be a "real risk" that significant harm will result from 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.

[18] In considering whether there exists a "real" risk of significant harm as a result of this incident I considered P2012-ND-09, P2011-ND-011 and P2011-ND-012. In these cases it was decided that a real risk of significant harm to individuals existed as a result of a hacker gaining unauthorized access to personal information. The personal information involved included names, email addresses and language of preference or country. An important factor in determining a real risk of significant harm existed in

these cases was the large number of affected individuals, which increased the risk of phishing.

[19] Based on the above and given the circumstances of this incident, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. The personal information involved was accessed by an individual with nefarious intent and could be used for phishing. This factor combined with the large number of affected individuals involved in this incident and the fact that some of these individuals may be under the age of 18 contributed significantly to my decision.

V. Decision

[20] I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation") and to provide me with written confirmation that it has done so by October 11, 2013.

Jill Clayton
Information and Privacy Commissioner