ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-04

TRION WORLDS INC.

February 21, 2012

(Case File #P2043)

I. Introduction

[1] On December 21, 2011, I received a report from Trion Worlds Inc. ("Trion" 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 Trion 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 Trion 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 Trion 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 December 21, 2011, I received a written report from Trion describing an incident involving the unauthorized access to personal information that resulted when unauthorized intruders gained access to a Trion account database.

[8] On December 22, 2011, my Office contacted Trion to request that it provide additional information concerning the incident, in order for me to determine whether to require Trion to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and e-mails between December 22, 2011 and February 14, 2012.

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

- The database breach occurred September 7, 2011 and continued to September 13, 2011. The breach was discovered conclusively on December 7, 2011 after learning that the account of a Trion employee had been compromised. An investigation was launched regarding the scope of the intrusion at that time.
- Information relating to 3.3 million accounts was contained in the affected server. Of those accounts, 11,411 accounts relate to Alberta, and of those 11,411 accounts, 242 indicated an age of under eighteen (18) in their profile.
- The personal information at issue includes the following:
    - First and last name;
    - Date of birth;
    - E-mail address;

    - Country of residence;
    - Name on credit/debit card;
    - First and last four digits of credit and debit card;
    - Expiration date of credit/debit card;
    - Billing address;
    - Password;
    - PayPal e-mail address (if applicable); and,
    - Secondary verification information (secret question and answers to assist in password recollection).
- Although they were encrypted, in this case, passwords were accessed by the attackers. Once the hacker could access the password, they would be able to log in to the company's account website and view the personal information of the affected individuals.
- Trion does not store full credit/debit card information, and uses third party payment processors. Trion reported that it is "relatively confident" that no credit/debit card full numbers were accessed.
- The attack appears to have originated in China, and continued through Japan and Korea.
- Monitoring systems were in place at the time of the breach. One of the alerts was missed by Trion's security team.
- Following the incident, Trion sent an e-mail notification to the account holders. The notification was sent on December 22-23, 2011.

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 Trion 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 Trion 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 Trion notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the individuals 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] Trion noted that without full access to credit card numbers in this case, the personal information at issue is not highly sensitive. In its assessment of harm, Trion stated that although the encryption for the user passwords had been compromised, there was no evidence that the encryption of the credit/debit card information had been breached. As such, Trion believes there is minimal risk of significant harm to the affected individuals. Trion stated that it regularly advises its players to be vigilant for potential phishing attempts and monitors phishing attempts.

[13] Unauthorized access to or disclosure of the personal information at issue could result in phishing attempts, and with access to name and date of birth, identity theft, which, in my view, is a significant harm. Also, it is possible that individuals use the same password and username for other accounts. Knowledge of this by the attackers could lead to a breach of other sources or accounts of personal information which is a significant risk.

[14] In order for me to require Trion to notify the affected individuals, 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 the attack itself, as stated by Trion, was a professional hack. This suggests malicious intent on the part of the hacker(s). Additionally, the attacker(s) were able to access the personal information of a very large number of individuals. While Trion stated it does monitor for phishing attempts, if it is notified after the fact that an attempt has been made, such action does not prevent an attempt from occurring.

[16] Given the information reported by Trion, 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: the attack was done with malicious intent; the information at issue is highly sensitive; and, there were a very large number of individuals affected by this breach.

V. Decision

[17] Based on the information reported to me by Trion, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Trion to notify affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation*.

[18] I understand Trion has already notified the affected individuals by way of e-mail sent on December 22-23, 2011, however, the notice does not contain the requirement pursuant to 19.1(1)(b)(ii). I order that Trion notify the affected individuals who are residents in Alberta of the time period during which their information was accessed in accordance with s. 19.1(1)(b)(ii) by March 7, 2012.

Jill Clayton
Information and Privacy Commissioner