ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-018

SONY ONLINE ENTERTAINMENT LLC

July 27, 2011

(Case File #P1868)

I. Introduction

[1] On May 2, 2011, I received a report from Sony Online Entertainment LLC ("SOE" 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 SOE 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 SOE 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 SOE 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 May 2, 2011, I received a written report from SOE describing an incident involving the unauthorized access to personal information.

[8] Numerous telephone conversations and e-mail exchanges between May 3, 2011 and July 7, 2011 were conducted between my Office and SOE to request that it provide additional information concerning the incident, in order for me to determine whether to require SOE to notify individuals under subsection 37.1(1) of PIPA.

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

- On May 1, 2011 SOE personnel discovered evidence that between April 16 and April 17, 2011 customer data may have been taken by an attacker during an unauthorized and illegal attack on its network. Following discovery of the incident, all SOE game services were temporarily turned off as SOE continued its investigation into the breach.

- SOE reported that the intruder issued a query that was designed to query specific data fields for each of the SOE network's approximately 24.6 million registered user accounts containing any customer information. The number of potentially affected Canadians is 956,419, and potentially affected Albertans accounts is 31, 463. SOE reports that there are approximately 170,000 affected Canadian SOE accounts registered with an age under 18 years at the time of the breach.

- SOE confirms there currently is no evidence that any payment card data was either accessed or stolen. The personal information known to have been accessed included:

    - Name
    - E-mail address
    - Birthdate

- Login name
- Hashed Password
- Country identifiers

- SOE stated that it had strong security measures in place at the time of the incident, and employs robust information security measures to protect customer data being handled on extremely complex networks. Sony utilizes a global framework for providing policies to its group companies based on ISO 27001, and SOE maintains restricted access to data on the network.

- At present, SOE is continuing to investigate the unauthorized intrusion. Third party security firms are participating in this investigation. In addition, SOE is working with the Federal Bureau of Investigation in the United States. SOE has taken numerous precautions to prevent a future incident, and these steps were in progress prior to the breach occurring:
  - Additional automated software monitoring and configuration management to help defend against new attacks;
  - Enhanced level of data protection and encryption;
  - Enhanced capabilities to detect software intrusions within the network, unauthorized access and unusual activity patterns; and
  - Implementation of additional firewalls.

- On May 2, 2011, SOE began notifying consumers via e-mail, website postings, and through the media. In addition, SOE also notified consumer reporting agencies Equifax, Experian, and TransUnion of the unauthorized intrusion.

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 SOE 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 SOE to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident. Numerous factors are considered when determining whether a real risk of significant harm has occurred, which include but in no way are limited to: the magnitude of the breach, that is the number of affected individuals, the maliciousness of the breach including whether or not personal information was hacked and stolen, the sensitivity of the information and the harm that may result. Each breach must be assessed based on the circumstances of that particular case.

[11] In order for me to require that SOE notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the affected 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] In this case, the personal information at issue is of moderate sensitivity as it includes numerous data elements such as: name, e-mail address, birthdate and country identifiers. Given that login names and passwords were hashed, which is a form of encryption, this information is low sensitivity.

[13] SOE noted that the likelihood that harm that could result from the unauthorized access to or disclosure of this information is relatively low. Although not extremely sensitive data elements on their own, in combination the information accessed could be used to commit identity theft as well as spear phishing attacks.

[14] In order for me to require SOE to notify its affected customers, however, there must also be a "real risk" of significant harm to the individual 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] As noted, SOE stated that the likelihood that harm could result is relatively low. SOE stated that without more sensitive identifiers including credit card information, which was not accessed, the risk of identity theft or fraud is minimal. Moreover, almost immediately following discovery of the unauthorized intrusion, SOE notified its customers as well as the media of the breach. SOE offered to provide its customers with a complimentary offering to assist users in enrolling in identity theft protection services and/or similar programs.

[16] However, whether or not an organization has already notified affected individuals is not a factor for consideration in determining whether there is a real risk of significant harm. Prior notification, assuming it is done in accordance with s. 19 of the PIPA Regulation, may relieve an organization of a requirement to notify again, but it does not affect whether the breach incident itself is considered a real risk of significant harm to affected individuals. This Office has already published numerous decisions where the fact that an organization had already notified affected individuals had no bearing on whether there was a real risk of significant harm.

[17] I further note that approximately 170,000 affected Canadian accounts are registered as being under 18 years of age. Section 61(1)(b) of PIPA recognizes that individuals under 18 years of age may have the ability to understand the nature of and consequences of exercising their rights under PIPA, so by singling out youth affected by this breach, I do not mean to indicate that youths are automatically afforded a different status or treatment under the Act. However, given the number of affected individuals under 18, I am of the opinion that a portion of these youths may be particularly vulnerable to the risks created by this breach. The youth of many of the affected individuals may make them more vulnerable to significant harms such as identity theft or fraud and I consider this to be a real risk.

[18] Given the information reported by SOE, I have decided that there is a real risk of significant harm to individuals as a result of this incident. The information at issue is of moderate sensitivity, and I have based my decision on the following factors: the type of information involved could be used for spear phishing attempts as well as to commit identity theft, which is a significant harm, and I have also considered the youthful ages of many of the affected individuals.

V. Decision

[19] Based on the information reported to me by SOE, I have concluded there is a real risk of significant harm to individuals as a result of this incident, and I require SOE to notify the affected individuals. I understand SOE has already notified all of the affected individuals by way of an email sent on May 2, 2011. I further note that SOE's notification was compliant with section 19.1 of the PIPA Regulation, and therefore, I will not require SOE to notify affected individuals again. I commend SOE for its cooperation and helpful submissions to this Office. Although a breach cannot always be prevented, an organization can certainly mitigate risks though responding to the situation and notifying affected individuals.

Frank Work, Q.C.
Information and Privacy Commissioner