ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-16

Indie Research, LLC

May 30, 2012

(Case File #P2103)

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 April 27, 2012, Indie Research, LLC (the "Organization") provided notice of an incident involving the 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 headquartered in the State of New Jersey, in the United States of America ("USA"). The information involved in the incident was stored on a server in the State of Massachusetts, USA. The Organization collected information from individuals who subscribed to an investment newsletter offered by the Organization. Alberta residents were among those individuals that subscribed to the newsletter.

[6] The Organization reported the incident involved the following information:

- The subscribing individual's:
  - first name or initial and last name,
  - credit card number and expiry date,
  - email and billing addresses, and
  - login information to enable access to the Organization's website.

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

[8] 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 was collected from residents of Alberta.

III. Background

[9] On May 7, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization on May 9, 2012.

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

- Between April 3, 2012, and April 7, 2012, the personal information on the Organization's server was hacked into providing access to unauthorized third parties.
- The incident was discovered by the Organization on April 11, 2012.

- The incident involved a total of 3146 individuals.
- Twelve of those individuals are Alberta residents (the "Affected Individuals").
- The personal information involved in the incident was collected in 2004 and 2005.
- The validity of the credit card numbers is unknown given the age of the data.
- The incident was reported to a number of law enforcement agencies, the merchant bank processor, credit bureaus, and the credit card companies involved.
- The Organization is in the process of reviewing and updating its security measures to prevent future incidents.
- The Organization sent a letter on April 24, 2012, to the Affected Individuals regarding the incident.

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

[11] 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] The personal information at issue is highly sensitive. It includes the names, email and billing addresses, full credit card numbers and credit card expiry dates of the Affected Individuals. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft or fraud. In my view, this is a significant harm.

[15] 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.

[16] The Organization reported the incident did not pose a significant risk of "additional harm" due to the age of the credit card information, the limited number of Affected

Individuals, and the fact that more sensitive information, such as social insurance numbers, did not appear to be accessed. Further, it had not received any reports of identity theft or fraud from the individuals involved in the incident.

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

- the age of the data,
- the personal information was accessed by means of a hacker with malicious intent, and
- the personal information is highly sensitive and could be used to commit identity theft or fraud despite its age or validity.

[18] In Breach Decision P2011-ND-034, Commissioner Work decided that, despite the age of the credit card numbers breached in that case, a real risk of significant harm existed to the affected individuals and required notification. The personal information at issue in that case was the name, billing and email addresses, credit card number and expiry date of individuals collected between the years 2001 to 2006. The organization checked the validity of the credit card numbers and only notified individuals whose credit card information had not expired. Commissioner Work determined that it would not be difficult for an individual who wished to engage in identity theft to derive new expiry dates from expired credit card information since expiry dates occur in predictable cycles. Commissioner Work decided that individuals with credit card information that had expired were also at a real risk of significant harm and required the organization to notify those individuals.

[19] Based on the information reported to me by the Organization, I have decided that there is a real risk of significant harm to the Affected Individuals as a result of this incident.

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").

[21] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in a letter sent on April 24, 2012. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner