ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-043

AARON'S INC.

November 1, 2011

(Case File #P2006)

I. Introduction

[1] On October 18, 2011, I received a report from Aaron's Inc. ("Aaron's" or the "Organization") of an incident involving the loss of and 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 Aaron's 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 Aaron's 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 Aaron's 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 October 18, 2011, I received a written report from Aaron's describing an incident involving the loss of and unauthorized access to personal information.

[8] On October 24, 2011, my Office contacted Aaron's to request that it provide additional information concerning the incident, in order for me to determine whether to require Aaron's to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and e-mail correspondence between October 24, 2011 and October 26, 2011.

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

- On September 26, 2011, an Aaron's franchisee store was burglarized in Freso, California. The thieves stole an assortment of goods, including TV's, computers, and electronic gaming devices.
- Among the goods stolen from the store was a computer that was used in the store's day–to-day operations. It was determined that this stolen computer contained a file with the personal information of customers who owed payments outstanding to the Organization. There were a total of 695 affected Albertans that had their personal information in this file. The personal information at issue in this file included:
    - Customer name, and
    - Customer Social Insurance number

- Security access controls on the computer that was stolen were limited to password protection on the server. There was no encryption or password protection on the file that maintained the personal information of the affected individuals.
- At the time the incident occurred, Aaron's had monitoring and alarm systems in place at its store. The Organization is currently reviewing its procedures as a response to the incident and may adjust accordingly.
- Aaron's reported the incident to law enforcement, and is continuing with its own internal investigation. The stolen computer has not been recovered.
- Aaron's notified the 695 affected Albertan's of the incident on October 24, 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 Aaron's 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 Aaron's 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 Aaron's notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the customers 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 high sensitivity as it includes customer name and their social insurance numbers. The Organization stated the likelihood that harm would result from this incident was low in terms of probability because the computer, like all of the other goods stolen, was taken for the value of the hardware and not the data. That said, I believe that personal information, particularly social insurance numbers, are highly sensitive personal information and are of value to those who commit theft. The type of harm that could result from the unauthorized access to or disclosure of this personal information is identity theft, which, in my view, is a significant harm.

[13] In order for me to require Aaron's to notify its affected customers, however, there must also be a "real risk" of significant harm to the customers 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.

[14] In deciding whether there exists a "real risk" of harm in this case, I considered that the personal information is sensitive in nature and could be used to commit identity theft. Security access controls to obtain access to the personal information maintained on the computer were minimal. While the Organization stated that the merchandise stolen, including the computer with the personal information on it, was taken for the value of its

hardware, the incident was committed by thieves with malicious intent who were looking to make money from stolen items.

[15] Given the information reported by Aaron's, 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 type of information involved could be used to commit identity theft, which is a significant harm; the incident is the result of a theft, and technical access controls to the personal information were minimal.

V. Decision

[16] Based on the information reported to me by Aaron's, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Aaron's to notify the affected individuals. I understand Aaron's has already notified the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of letter sent on October 25, 2011; therefore, I will not require Aaron's to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner