ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-01

ATB Financial

January 10, 2013

(Case File #P2226)

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 17, 2012, ATB Financial (the "Organization") provided notice of an incident involving the loss of 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 registered and operating in Alberta. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

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

- name,
- investment account number,
- date of birth,
- social insurance number ("SIN"),
- address, and
- phone number.

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

III. Background

[8] On December 19, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization on December 19, 2012.

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

- On November 5, 2012, a vehicle belonging to an ATB Securities Associate ("the Associate") was broken into while it was parked in the Organization's parking lot for the period of 1 hour that evening. The Associate left a briefcase containing the personal information belonging to 2 individuals ("the Affected Individuals") as well as numerous personal effects in his or her vehicle.
- The Organization reported the theft to the Calgary Police Service.
- The briefcase was returned to the Associate by mail over the first weekend of December, 2012. All of the contents of the bag were accounted for except the envelope containing the personal information.

- The Affected Individuals were notified by telephone on November 21, 2012.
- The Associate entered notes on the Affected Individuals' investment accounts to notify other Associates of the nature of the theft and to exercise caution with the accounts. Further, the Organization flagged the other accounts belonging to the Affected Individuals as a precaution.

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

[10] 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.

[11] 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.

[12] 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.

[13] The Organization reported that in its opinion the incident did pose a risk of significant harm because the information was stolen and given that this type of personal information is highly sensitive, it may result in identity theft or fraud which may lead to financial losses for the Affected Individuals.

[14] The personal information at issue is highly sensitive. It includes the name, SIN, date of birth, address, phone number, and account number of the Affected Individuals. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft and fraud. In my view, these are significant harms.

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

- The personal information is highly sensitive.

- The type of information involved could be used to commit identity theft and fraud.
- The information was stolen and has not been recovered.
- The bag was returned with all the contents except the envelope containing the personal information.

[17] Cases P2010-ND-006, P2011-ND-028, and P2012-ND-01 involved breaches of similar circumstances in which highly sensitive personal information of a similar nature to this incident was stolen and not recovered. In these cases, it was decided that a real risk of significant harm, identity theft and fraud, existed to the Affected Individuals.

[18] Based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the Affected Individuals as a result of this incident.

V. Decision

[19] I require the Organization to notify the Affected Individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[20] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in a phone conversation on November 21, 2012. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner