ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-005

ALBERTA TREASURY BRANCHES, carrying on business as ATB FINANCIAL

February 22, 2011

(Case File #P1764)

I. Introduction

[1] On February 4, 2011, I received a report from ATB Financial (ATB) 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 ATB 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] ATB reported that the information at issue in this incident consisted of fifty customers' names and signatures, bank account numbers, the date, time, and details of their bank transactions.

[6] This is information about identifiable individuals and so qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

[7] In considering whether to require ATB to notify affected individuals, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

[8] On February 4, 2011, I received a written report from ATB describing an incident involving the unauthorized access of personal information.

[9] On February 14, 2011, my Office contacted ATB to request that it provide additional information concerning the incident, in order for me to determine whether to require ATB to notify individuals under subsection 37.1(1) of PIPA. My Office received ATB's response on February 14, 2011.

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

- On January 4, 2011 at approximately 3:00 p.m. "robbers walked" into the ATB branch located in Onoway, Alberta.
- The robbers stole some cash and an envelope from the Customer Service Representative (CSR) station.
- Inside the envelope, there were customer service application generated receipts containing fifty customers' names and signatures, bank account numbers, the date, time, and details of their bank transaction of January 4, 2011.
- ATB (Onoway) reported the incident to the RCMP in Stony Plain on January 4, 2011 and to the ATB head office.
- Subsequently, ATB notified forty-seven (out of 50) customers about the incident by telephone and the remaining three customers were notified by registered letter, dated January 24, 2011.
- ATB also provided a description of the personal information that was stolen during the incident to each customer and offered to change their bank account numbers, replace their cheques and monitor their accounts.
- ATB advised that the RCMP arrested the alleged robbers on January 21, 2011; however, ATB does not know whether the stolen information was recovered.

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

[11] Pursuant to section 37.1 of PIPA, I have the power to require ATB 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 ATB to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

[12] In order for me to require that ATB notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to that individual as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[13] In this case, the personal information at issue consists of the customers' names and signatures, their bank transaction of January 4, 2011, and bank account numbers. While an individual's name is not particularly sensitive information, the inclusion of the bank account number in connection with this information raises the sensitivity of the information to moderate to high sensitivity.

[14] In my view, the personal information in ATB's envelope could be used to cause significant harm to these individuals in the form of identity theft and/or fraud.

[15] As ATB noted, this is information that could be used for identity theft.

[16] In order for me to require ATB to notify the customers, however, there must also be a "real risk" of harm to the individual as a result of the incident. This standard does not require that 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.

[17] In deciding whether there exists a "real risk" of harm in this case, I considered that ATB immediately informed the RCMP of this incident. However, the customers' personal information was stolen and has not been recovered. Given the sensitivity of the personal information of the customers at issue, and the fact that the information was stolen, and not recovered, I believe there is a real risk of significant harm to the fifty individuals whose personal information was in ATB's envelope stored at ATB (Onoway) on January 4, 2011.

V. Decision

[18] I understand ATB has already notified the affected individuals by telephone and registered letter about the incident involving the unauthorized access to personal information. However, section 37.1(1)(a) of PIPA gives me the power to require that ATB notify individuals "in a form and manner prescribed by the regulations". Therefore, I require ATB to notify the fifty affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, if it has not already done so.

Frank Work, Q.C.
Information and Privacy Commissioner