ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-009

CitiFinancial Canada Inc.

April 12, 2011

(Case File #P1787)

I. Introduction

[1] On March 11, 2011, I received a report from CitiFinancial Canada Inc. (Citi) of an incident involving the unauthorized disclosure of 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 Citi 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 Citi is an "organization" as defined in section 1(1)((i)(i) of PIPA which operates in Alberta, and the information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

[6] In considering whether to require Citi 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 March 11, 2011, I received a written report from Citi describing an incident involving the unauthorized disclosure of personal information.

[8] On March 31, 2011, my Office contacted Citi to request that it provide additional information concerning the incident, in order for me to determine whether to require Citi to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided by telephone on March 31, 2011.

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

- On March 3, 2011 an employee of Citi discovered an error in regard to two mailings of February 24, 2011;
- Citi reported that these mailings contained T4A statements of two retired Citi employees which had been mailed to two other retired employees of Citi in error;
- The T4A statement sets out pension and retirement income. It includes the name of retiree, mailing address, social insurance number, type of income, amount paid, and income tax deducted;
- On March 9, 2011, letters of notification were couriered to the affected retirees;
- Citi's notification letter described the incident, informed the affected retirees that Citi had sent a letter asking the individuals who had received the T4A statement in error to return the information to Citi without making copies. The affected retirees were also offered 12 months of credit monitoring services;
- Citi is in the process of retrieving the T4A statements from the individuals who received the information in error.

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 Citi 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 Citi 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 Citi notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the retired Citi employees 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 my view, the personal information of the two retired Citi employees contained in the mailings is of high sensitivity as it includes the retirees' names, addresses, social insurance numbers, type of income, amount paid, and income tax deducted.

[13] This is information that could be used to cause significant harm to individuals, and provides comprehensive individual profiles that could be used for identity theft and/or fraud.

[14] Citi also noted that the type of harm that could result from the unauthorized disclosure of this information is identity theft, which, in my view, is a significant harm.

[15] In order for me to require Citi to notify its retired employees, however, there must also be a "real risk" of harm to these retirees 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.

[16] In deciding whether there exists a "real risk "of significant harm in this case, I considered that Citi notified the affected individuals six days after it had discovered the incident. However, given the sensitivity of the personal information of the two retirees at issue, I believe there is a real risk of significant harm to those individuals whose T4A statements were mailed to two individuals not authorized to receive the information.

V. Decision

[17] I understand that Citi has already notified the affected retirees by way of its March 9, 2011 letter. However, section 37.1(1) (a) of PIPA gives me the power to require that Citi notify the affected individuals "in a form and manner prescribed by the regulations". Therefore, I require Citi to notify the affected retirees 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