ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-013

H&R BLOCK

May 11, 2011

(Case File #P1854)

I. Introduction

On April 13, 2011, I received a report from H&R Block Canada Inc. ("H&R Block") of an incident involving the loss of, and possible unauthorized access to and disclosure of, personal information of individuals in Alberta. Based on the information reported to me, I have decided that there is a real risk of significant harm to those individuals as a result of the incident, and therefore I require that H&R Block notify those individuals to whom there is a risk of significant harm.

II. Jurisdiction

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.

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 signification 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.

H&R Block reported that the information at issue in this incident consists of client's name, social insurance number, and notice of assessments from the Canada Revenue Agency ("CRA").

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

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;

I have jurisdiction in this matter because H&R Block is an "organization" as defined in s. 1(1)(i) of PIPA, and the information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

In considering whether to require H&R Block to notify affected individuals, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

On April 13, 2011, I received a written report from H&R Block describing an incident involving the loss of, and possible unauthorized access to and disclosure of, personal information.

On April 27, 2011, my Office contacted H&R Block by telephone and spoke with its VP Franchise Operations and Privacy Officer, to request that it provide additional information concerning the incident, in order for me to determine whether to require H&R Block to notify individuals under subsection 37.1(1) of PIPA.

In summary, the circumstances of the incident reported to me are as follows:

- Over the course of the past year, a number of clients of H&R Block contacted the Organization noting a change of address. This change of address was entered into the H&R Block database.
- On March 22, 2011, a set of client letters were mailed to 58 clients who had had a change of address in the past year.
- On March 30, 2011, a software issue that lead to the breach was discovered. Realization that the breach was related to clients that had noted a change of address was discovered on April 2, 2011.
- The breach was a mailing of CRA letters to the correct name, but incorrect address.

- The incident was discovered when IT staff noted unexpected results when running a query of the client database which is housed at H&R Block's head office in Calgary.
- The breach was sourced to a software issue and how it incorrectly treated certain converted client files (clients who had had a change of address). The affected records showed incorrect address updates resulting in the use of an older address from the client's history of records.
- H&R Block indicates that it believes there is a medium risk of harm with respect to the potential or likelihood of identity theft for the affected clients. It contends that in order for any significant harm to occur, that an individual would have to open the envelope they received in error (addressed to that individual's current place of residence, and addressed to them in name), and then use the information for fraudulent purposes.
- With regards to steps taken by H&R Block to mitigate the incident, the organization notes that all clients whose information was mailed to another address that has not already been returned unopened will be contacted by telephone. If those clients are not reachable by phone, H&R Block will send them a letter. Additionally, where clients are unreachable via phone, or do not respond to letters mailed to them detailing the incident, H&R Block indicated to this Office that they would go to the residence where the letters of assessment were sent in error and try to obtain the mail of their clients.
- H&R Block is offering each client affected one year of credit monitoring and identity theft protection.
- Some of the letters are coming back to H&R Block unopened via returned mail from Canada Post.
- During this phone conversation, information regarding an update on the status of the organization's number of returned (unopened) envelopes was requested.

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

Pursuant to section 37.1 of PIPA, I have the power to require H&R Block 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 H&R Block to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

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

In this case, the personal information at issue is of moderate to high sensitivity as it includes names, addresses, Social Security numbers, and income information regarding assessments from the CRA.

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

In order for me to require H&R Block to notify individuals, however, there must also be a "real risk" of harm to individuals 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.

H&R Block has determined that the incident occurred as a result of a software issue where client addresses were not accurately updated. Once a query was performed on the client database, and the issue was identified, H&R Block took steps to recover the information. However, at this time, and despite an ongoing investigation, all of the misdirected client CRA assessments have not yet been recovered by the organization. Given that the mail-out occurred on March 22, 2011, the letters have been out for approximately six weeks.

Given the sensitivity of the information at issue, and considering that not all the client letters have been returned unopened back to H&R Block, I believe there to be a real risk of significant harm in this case.

V. Decision

Based on the information reported to me by H&R Block, I have concluded there is a real risk of significant harm to individuals as a result of this incident, and I require H&R Block to notify individuals.

I understand H&R Block has begun the process of notification at this time.

Frank Work, Q.C.
Information and Privacy Commissioner