ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-027

TRANSAMERICA LIFE CANADA

August 30, 2011

(Case File #P1960)

I. Introduction

[1] On August 17, 2011, I received a report from Transamerica Life Canada ("Transamerica" or "the Organization") of an incident involving the unauthorized access to or disclosure of personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to the affected individuals as a result of the incident, and therefore I require that Transamerica 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 Transamerica 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 Transamerica 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 August 17, 2011, I received a written report from Transamerica describing an incident involving the unauthorized access to or disclosure of personal information.

[8] On August 18, 2011, my Office contacted Transamerica to request that it provide additional information concerning the incident, in order for me to determine whether to require Transamerica to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of email correspondences between August 18, 2011, and August 22, 2011.

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

- On May 24, 2011, Transamerica processed a request for a partial withdrawal of funds for the sum of $75,000 from a policy held jointly by two Alberta residents. The funds were wire transferred to a bank account in their names pursuant to the request.
- As a result of suspicion raised by the bank on May 27, 2011, Transamerica contacted the policyholders and the policyholders confirmed that they did not request the withdrawal.

- Transamerica retroactively reversed the withdrawal on June 24, 2011, with an effective date of May 24, 2011, to ensure the policyholders did not experience any loss.
- Transamerica submits that it is not known how or from where the personal information of the policyholders was obtained by the individual(s) who used it to request the withdrawal. Transamerica is continuing to conduct an internal investigation into the circumstances of the withdrawal. The police are also investigating this matter.
- The following details were included in the withdrawal request: policy number, names of both policyholders, home address of the policyholders, a facsimile of signatures of the policyholders, a social insurance number of one policyholder and a blank personal cheque with the names and address of the policyholders pre-printed on the cheque with the bank account number to which the withdrawal was to be deposited.
- Transamerica notified the policyholders both by telephone and in writing with respect to the unauthorized withdrawal and recommended they take steps to advise their bank and the credit bureau of the incident.
- Transamerica states it has strengthened its internal control procedures concerning request for withdrawals.

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 Transamerica 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 Transamerica 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 Transamerica notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to those 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.

[12] In this case, the personal information at issue is of moderate to high sensitivity as it includes name and address of the policy holders, social insurance number, and information concerning the insurance policy that permitted the partial withdrawal of the funds.

[13] Transamerica also noted that the type of harm that could result from the unauthorized access to or disclosure of this information is identity theft, which, in my view, is a significant harm.

[14] In order for me to require Transamerica to notify the policyholders, however, there must also be a "real risk" of significant harm to the 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. Further, there must be a cause and effect relationship between the incident and the possible harm.

[15] In deciding whether there exists a "real risk" of harm in this case, I considered that it is unknown at this time how the personal information of the policyholders was obtained that permitted the unauthorized withdrawal to take place. I also considered the sensitivity of the data elements and the fact that the risk had already materialized as someone actually did use the information to access the insurance policy funds.

[16] Given the information reported by Transamerica, I have decided that there is a real risk of significant harm to the two policyholders as a result of this incident. I have based my decision on the following factors: the type of information involved was purportedly used and could be used in the future to commit identity theft, which is a significant harm, the fact that it is still unknown how the personal information of the policyholders was obtained and the person(s) responsible for the unauthorized withdrawal request has not been identified by either Transamerica or the police as of the date of this decision.

V. Decision

[17] Based on the information reported to me by Transamerica, I have concluded that there is a real risk of significant harm to the two policyholders as a result of this incident and I require Transamerica to notify those individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation*.

[18] I understand Transamerica has already notified the individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of direct conversations with the policyholders and correspondence with the policyholders' legal counsel sent on June 29, 2011, and August 4, 2011. Based on this information provided to me by Transamerica, I do not require Transamerica to notify the individuals again.

Frank Work, Q.C.
Information and Privacy Commissioner