ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-022

Empire Life Insurance Company

July 13, 2011

(Case File #P1914)

I. Introduction

[1] On June 17, 2011, I received a report from Empire Life Insurance Company ("Empire Life" or the "Organization") 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 Empire Life 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 Empire Life 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 Empire Life 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 June 17, 2011, I received a written report from Empire Life describing an incident involving the unauthorized disclosure of personal information. On July 12, 2011, my Office contacted Empire Life via telephone to clarify specifics concerning the incident.

[8] The circumstances of the incident reported to my Office are as follows:

- On May 3, 2011 one term insurance policy file was sent via courier to the wrong address. The breach was caused by selecting the incorrect receiver from the FedEx Shipping system.
- The incident was discovered on June 6, 2011 when the recipient who had received the file in error contacted Empire Life to advise that the recipient had received a file from the Organization in error. The file was sent to the recipient's address, but was not addressed to the recipient. The recipient opened the package despite the fact it was not addressed to her in name.
- The number of affected Empire Life clients affected as a result of the breach is two (2).
- All information contained in the file was in paper format and included the following personal information of the two Empire Life clients:
    - Name
    - Address
    - SIN
    - Policy number
    - Medical information
    - Visa number (from 1995)
    - Driver's license number
    - Bank account number
- Following notification to Empire Life that the recipient had received the file in error, the recipient returned the file to Empire Life after Empire Life organized for

FedEx to pick up the package at the recipient's residence. The Organization confirmed that it received the file back in its entirety.

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

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

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

[11] In this case, the personal information at issue is of high sensitivity as it includes name, SIN, medical information, and bank account details. This type of personal information could be used to commit identity theft while the loss of medial information could cause hurt, humiliation, or damage to one's reputation.

[12] Empire Life 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.

[13] In order for me to require Empire Life to notify its clients, however, there must also be a "real risk" of significant harm to the clients 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.

[14] In deciding whether there exists a "real risk" of significant harm in this case, I considered that the personal information at issue in this case is of high sensitivity and includes SIN, medical information, and bank account information of individuals. This information could be used to commit identity theft. In addition the information at issue was sent via courier to the wrong recipient on May 3, 2011, and while that recipient did notify the Organization of the error, the recipient did not get in contact with someone at Empire Life until June 6, 2011. As such, the personal information of the two Empire Life clients remained misdirected for just over one month.

[15] Given the information reported by Empire Life, I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the following factors: the type of information involved could be used to commit identity theft, which is a significant harm; and, the amount of time the information remained misdirected before it was returned to the Organization.

V. Decision

[16] Based on the information reported to me by Empire Life, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Empire Life to notify individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation*. I have received confirmation in writing that Empire Life has already notified those clients affected by the breach, therefore, I do not require Empire Life to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner