ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-32

Sun Life Assurance Company of Canada

July 2, 2013

(Case File #P2182)

I. Introduction

[1] 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.

[2] On October 23, 2012, Sun Life Assurance Company of Canada (the "Organization") provided notice of an incident involving the loss of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[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] The Organization is licensed under the Alberta *Insurance Act* to carry on business in Alberta. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The Organization reported the incident involved the following information collected on group benefits enrolment forms for 49 Alberta customers:

- name,
- gender,
- address,
- date of birth,
- language,
- marital status,
- plan information (single or family coverage selection, class or plan, coverage date, location billing group name and number, and plan member identification number),
- employment information (occupation, salary, status, and date as new hire or rehire),
- beneficiary information (name, relationship to customer, and benefit description),
- spouse information (name, date of birth, gender, and employer benefit plan if applicable), and
- child or children information (name, date of birth, gender, and indication if the child is a student)

[8] This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[9] On November 29, 2012, and January 3, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between December 3, 2012, and January 7, 2013.

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

- On October 9, 2012, a benefit consultant notified the Organization that group benefit enrolment forms mailed by the Organization on September 12, 2012, had not been received.
- The Organization and benefit consultant searched for the forms in their respective offices and did not find them.
- The matter was reported to Canada Post on October 22, 2012. Canada Post advised that the package containing the forms did not appear in its "undelivered" database.
- The forms have not been recovered.
- A letter notifying customers of the incident was sent on October 23, 2012.
- Customers were offered a one year credit monitoring subscription.

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

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

[12] Pursuant to section 37.1 of PIPA, I have the power to 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." In determining whether or not to require the Organization to notify the affected individuals, I must consider if there is a "real risk of significant harm" to the affected individuals as a result of the incident.

[13] In order for me to require that the Organization notify the affected 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. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[14] The Organization reported the incident did not pose a real risk of significant harm to the affected individuals. The Organization submitted that more sensitive information, such as social insurance numbers or medical information was not contained on the forms.

[15] In my view, the personal information at issue is moderately sensitive and could be used to commit identity theft or fraud. Beneficiary information could also be used to cause harm in the form of hurt, humiliation, and damage to relationships. In my view these are significant harms.

[16] In order for me to require the Organization to notify the affected individuals, there must also be a "real risk" of significant harm to the affected 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. There must be a cause and effect relationship between the incident and the possible harm.

[17] The Organization recognized that if the forms fell into the wrong hands for illicit purposes there would be a real risk of significant harm for identity theft or fraud. It identified the risk as moderate.

[18] I have decided that there is a real risk of significant harm, in the form of identity theft and/or fraud, to the affected individuals as a result of this incident. The nature and amount of personal information involved, that the information was lost and has not been recovered, together with the Organization's inability to confirm how the information was lost contributed significantly to my decision.

V. Decision

[19] I require the Organization to notify the affected individuals in accordance with section 19.1(1) of the *Personal Information Protection Act Regulation* (the "Regulation").

[20] I understand the Organization notified customers of the incident in a letter dated October 23, 2012. The letter is in accordance with the Regulation. As a result of sending the letter directly to customers, their spouses and children were indirectly notified of this incident. Therefore, I will not require the Organization to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner