ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-10

Sun Life Assurance Company of Canada

March 26, 2013

(Case File #P2250)

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 February 5, 2013, Sun Life Financial (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* and is recognized as carrying 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 RRSP income statements (the "Statements") which contain the following information of its members:

- name,
- address,
- social insurance number ("SIN"),
- group RRSP contract number, and
- 2012 RRSP withdrawal amount and related income tax deduction.

[7] The information at issue qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On February 19, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between February 19 and February 26, 2013.

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

- On January 17, 2013, the Organization mailed the Statements to its members.
- The Organization determined there was an error in the mail production file. This caused the incorrect printing of addresses on 19 envelopes. Six of the 19 envelopes were delivered to the proper member. Two of the 19 envelopes were returned to the Organization. Eleven of the 19 envelopes were not delivered to the addressee or returned to the Organization. These envelopes have not been recovered.

- The Organization notified the 11 members whose envelopes were not returned to the Organization (the "Affected Individuals") of the incident by letter on February 1, 2013.

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

[10] 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.

[11] 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.

[12] 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 Affected 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.

[13] The Organization reported the incident did pose a risk of significant harm because the information is highly sensitive and could expose the Affected Individuals to identity theft or fraud.

[14] In my view, the personal information at issue is highly sensitive. It includes names, addresses, SINs, and RRSP information of the Affected Individuals. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft and fraud. In my view, these are significant harms.

[15] 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.

[16] The Organization reported the incident did pose a "real risk" of significant harm to the Affected Individuals if the personal information at issue were to be obtained by someone with malicious intent.

[17] In deciding whether there exists a "real risk" of significant harm in this case to the Affected Individuals, I considered the following factors:

- The personal information is highly sensitive.
- The type of information involved could be used to commit identity theft and fraud.
- The information was lost and has not been recovered.

[18] In P2011-ND-006 and P2011-ND-037, highly sensitive personal information of a similar nature to the information involved in this incident was lost in transit via mail and not recovered. In these cases, it was decided that a real risk of significant harm, identity theft and fraud, existed to the Affected Individuals.

[19] In my view, the highly sensitive nature of the personal information involved in this incident, together with the fact it has been lost and not recovered creates a likelihood that the significant harm, identity theft and fraud, will occur to the Affected Individuals as a result of this incident.

[20] Based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the Affected Individuals as a result of this incident.

V. Decision

[21] I require the Organization to notify the Affected Individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[22] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in a letter sent on February 1, 2013. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner