ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-11

SUN LIFE ASSURANCE COMPANY OF CANADA

June 4, 2012

(Case File #P2077)

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 March 7, 2012, I received a report from Sun Life Assurance Company of Canada (the "Organization") of an incident involving the unauthorized access to or disclosure 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 registered as a corporation operating in Alberta. The incident occurred at the Organization's headquarters located in Ontario.

[6] The Organization reported the incident involved the following information:

- The name, home address, group policy number, certificate number, date of birth, and claims details of dental benefits of 54 claimants. Four of the claimants were from Alberta (the "Alberta Claimants").
- The name and details of dental benefits of the Alberta Claimants' family members (the "Family Members").

[7] I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA and the information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On March 12, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between March 12, 2012, and April 3, 2012.

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

- The Organization has a website where plan members can access their claim information.
- A system error occurred enabling some plan members the ability to access claim information of other plan members, including the Alberta Claimants and the Family Members.
- Access included the ability to view, download, and print the claim form.
- A plan member reported the error to the Organization on March 1, 2012.
- The Organization immediately shut down access to claim information on its website to fix the error.

- The Organization was able to determine what plan member viewed another plan member's information.
- The Organization contacted the plan members who viewed the wrong claim information. Only one person could be reached. This person agreed to delete the personal information and to destroy it if printed. The other three people could not be reached but were sent letters requesting their cooperation.
- The Organization has identified the error and is making changes to the system to prevent reoccurrence.
- The Organization notified the Alberta Claimants and the Family Members by phone and letter.

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 these 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 type of harm that could result to the affected individuals from the alleged incident is identity theft, or hurt, humiliation and damage to reputation if the personal information were to fall into the wrong hands.

[14] In Breach Notification Decision P2011-ND-006, Commissioner Work stated the following:

> "The loss of the medical information and other personal information such as name, address and telephone number would likely not cause significant harm to individuals. However, these data elements combined with an individual's date of birth could be used to commit identity theft, which is a significant harm."

[15] In the present case, the combination of personal information of the Alberta Claimants is highly sensitive. The type of harm that could result to these individuals from unauthorized access or disclosure to this personal information is identity theft. In my view, this is a significant harm.

[16] The personal information of the Family Members is of low sensitivity. In my view, this personal information cannot be used to cause significant harm to these individuals.

[17] 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.

[18] The Organization assessed the risk of harm as low due to its knowledge of the plan members who accessed the personal information and the efforts made to contact these individuals.

[19] For the Family Members, there is no risk of significant harm. Therefore, there is no real risk that significant harm will occur to an individual.

[20] For the Alberta Claimants, in deciding whether there exists a "real risk" of significant harm to these individuals, I considered the following factors:

- The personal information in combination is highly sensitive and could be used for identity theft.
- The Organization is aware that the Alberta Claimants' information was viewed and potentially copied or printed by another plan member.
- The Organization was unable to confirm with three of the plan members who viewed the personal information of the Alberta Claimants to confirm they have deleted or destroyed the personal information.

[21] In Breach Notification Decision P2012-ND-005, I determined where highly sensitive information is breached and not recovered or confirmed destroyed, the knowledge of who received the information does not mitigate a real risk of significant harm from occurring.

[22] In this case, the personal information breached of the Alberta Claimants is highly sensitive and for three of these individuals the personal information accessed has not been confirmed deleted or destroyed.

[23] Based on the information reported to me by the Organization, and considering the factors discussed above, I have decided there is a real risk of significant harm to the three Alberta Claimants whose personal information was accessed by plan members and not confirmed deleted or destroyed.

V. Decision

[24] I require the Organization to notify the three Alberta Claimants in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[25] I understand that the Organization already notified the three Alberta Claimants by way of phone and letter. However, the notification provided does not meet the requirements of section 19.1 of the Regulation. Section 37.1 (1)(a) of PIPA gives me the power to require that the Organization notify individuals in a form and manner prescribed by the Regulation. Therefore, I require the Organization to notify the three Alberta Claimants in accordance with section 19.1 of the Regulation, if it has not already done so.

Jill Clayton
Information and Privacy Commissioner