ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-040

SUN LIFE ASSURANCE COMPANY OF CANADA

November 30, 2011

(Case File #P2028)

I. Introduction

[1] On November 17, 2011, I received a report from Sun Life Assurance Company of Canada ("Sun Life" or the "Organization") of an incident involving the loss 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 Sun 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 Sun 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 Sun 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 November 17, 2011, I received a written report from Sun Life describing an incident involving the loss of personal information.

[8] On November 21, 2011, my Office contacted Sun Life to request that it provide additional information concerning the incident, in order for me to determine whether to require Sun Life to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls, e-mail, and fax correspondence between November 21, 2011 and November 29, 2011.

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

- On November 8, 2011, a Sun Life Financial Advisor (the "Advisor") reported the theft of her briefcase which contained her laptop and documents belonging to a Sun Life client. The briefcase was stolen from the Advisor's locked car from a parking lot in Edmonton, Alberta while the Advisor attended a meeting.
- The documents that were stolen contained the personal information of a Sun Life client and that client's beneficiary. The personal information at issue in the four documents stolen is:
    - A Portfolio Review which contained the client's name, address, date of birth, premium amounts and the type of policy including cash values;
    - A Policy Illustration which contained the client's name, date of birth, premiums and future projections of the policy;

    - A Client Information Sheet which contained the client's date of birth, e-mail address, home address, and phone numbers; and,
    - A Beneficiary Form which contained the client's name, policy number and beneficiary designations.
- The Advisor's car doors were locked at the time of the incident, but the thief broke the car window to gain access to the briefcase.
- Sun Life reports that the laptop was encrypted. All information contained on the laptop is protected by the hard drive encryption program, including any cached content. In a review of its audit logs, Sun Life was able to confirm that the last time the Advisor's laptop was accessed via the network was on November 7, 2011. This is one day before the theft of the briefcase. The Advisor has confirmed that she did not store and client personal information on the hard drive of her laptop, and that her only access to client personal information was via the network which was encrypted.
- Sun Life advised that it has full hard disk encryption in place so any personal information would not be accessible unless unauthorized individuals could authenticate through encryption.
- The Organization stated that it takes proper precautions to protect clients' information by implementing a security program with the following elements:
    - A Corporate Security Policy with supporting security standards and procedures governing the secure configuration, operation and maintenance of information systems and protection of confidential client information;
    - Mandatory security and privacy awareness training for all employees, including advisors;
    - Full encryption of all laptops and desktops;
    - Secure deletion of data from surplus computer hard drives prior to disposal;
    - Use of firewalls, encryption, Intrusion Detection System (IDS), two-factor remote authentication, hardened operating systems, anti-virus software, and other logical and physical security controls to protect systems and information from unauthorized access and misuse.
- The Advisor contacted the Sun Life client via telephone in an attempt to tell the client about the theft. In addition, a letter was sent to the client on November 16, 2011 advising the client of the incident.

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 Sun 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 Sun Life 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 Sun Life notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to that client 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 high sensitivity as it includes the client's name, address, date of birth, and beneficiary information.

[13] Sun 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. Given that the documents were stolen, a risk of significant harm exists if the client's personal information were to be used to commit identity theft.

[14] In order for me to require Sun Life to notify the client, however, there must also be a "real risk" of significant harm to the client 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 significant harm in this case, I considered that the personal information at issue is of high sensitivity, and that it was stolen. While there may be a low risk that any client data could be accessed through the network on the laptop given the encryption software in place, it is certainly probable that a thief could use the client personal information on paper to commit identity theft.

[16] Given the information reported by Sun Life, I have decided that there is a real risk of significant harm to an individual 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 that the personal information at issue was lost as a result of theft.

V. Decision

[17] Based on the information reported to me by Sun Life, I have concluded there is a real risk of significant harm to an individual as a result of this incident and I require Sun Life to notify the affected individual. I understand Sun Life has already notified the individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of letter sent on November 16, 2011; therefore, I will not require Sun Life to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner