ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-037

Sun Life Assurance Company of Canada

November 1, 2011

(Case File #P1987)

I. Introduction

[1] On September 22, 2011, I received a report from Sun Life Assurance Company of Canada ("Sun Life") 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 the affected individual as a result of the incident, and therefore I require that Sun Life notify the individual 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 September 22, 2011, I received a written report from Sun Life describing an incident involving the loss of personal information.

[8] On September 29, 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 the individual under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls between September 22, 2011 and October 28, 2011.

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

- On June 17, 2011, an applicant for term life insurance with Sun Life provided health information on a paramedical form. The health information was collected by a service provider for Sun Life: an insurance medical services company that had sent a health professional to collect the applicant's current and past medical information history on a paramedical form.

- The health professional usually sends completed paramedical forms to the service provider's office through Canada Post, but because there was a postal strike at that time, the service provider had instructed its health professionals to use couriers.

- The health professional put the applicant's paramedical form in a courier package that was clearly labelled and appropriately addressed to the service provider's

office. However, the courier package was a unique style pouch (provided by the courier company) that was usually used by the courier service provider to send blood and urine samples to another Sun Life service provider – a lab that that the service provider uses for analyzing physical paramedical evidence samples. Unfortunately, despite being properly addressed and labelled, the courier did not identify the package destination correctly through the waybill, and instead shipped it to the lab based upon a visual identification of the package.

- On June 24, 2011, the insurance medical services company took note that the expected paramedical form had not yet arrived.

- By June 27, 2011, the insurance medical services company notified Sun Life that the expected paramedical form had not yet arrived in its office and that searches conducted by the insurance medical services company, and two labs (including the lab where the courier had directed the package) had not found the package.

- The courier was able to confirm the package had been directed to one of the labs used by the insurance medical services company, but was unable to locate any confirmation of delivery to the lab.

- The lab has an imaging system to track all incoming packages, and upon review, it was unable to find any evidence that the package had been delivered to the lab.

- The personal information of the one affected individual includes the following:
    - Name;
    - Policy number;
    - Evidence number;
    - Date of birth;
    - Driver's license number;
    - Physician's name, clinic name and city;
    - Paramedical evidence including:
        - smoking, drinking and drug use information,
        - information about current and past health as it relates to cardiovascular, geno-urinary, respiratory, skin etc.
        - other data such as measurements, blood pressure readings, pulse and a urinalysis test.

- The insurance applicant was notified about the loss of personal information on August 17, 2011.

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 individual 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 a detailed medical history of the insurance applicant.

[13] Sun Life also noted that the type of harm that could result from the unauthorized access to or disclosure of this information included a high risk of identity theft and a moderate risk of hurt, humiliation, and damage to reputation as well as potential loss of business or employment opportunities. These are, in my view, significant harms.

[14] In order for me to require Sun Life to notify the affected individual, however, there must also be a "real risk" of significant harm to the individual 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 harm in this case, I considered that the personal information had not been located despite the extensive searches conducted by both the insurance medical services company and the lab. Although the evidence provided by the courier indicated the package had been misdirected to the lab, the courier could not confirm the lab had received it. The lab had processes in place to track all incoming packages, and it was unable to locate any evidence the package had been received. This indicates, in my view, that the package was never received by the lab, but was lost by the courier somewhere in transit.

[16] Given the information reported by Sun 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, or to cause hurt and humiliation to the individual given the extensive medical history, which are significant harms. I have also considered that the evidence indicates the package did not arrive at any destination, but was lost en route.

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 the 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 a letter sent on August 17, 2011; therefore I will not require Sun Life to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner