



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Sun Life Assurance Company of Canada (Organization)
Decision number (file number)	P2016-ND-21 (File #P2835)
Date notice received by OIPC	August 28, 2014
Date Organization last provided information	August 28, 2014
Date of decision	March 15, 2016
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The organization is required to notify those individuals pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is incorporated and operating in Alberta and is an “organization” as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved all or some of the following information about the individuals:</p> <ul style="list-style-type: none">• name,• address,• date of birth,• contract number and value, and• social insurance number <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

Description of incident	<ul style="list-style-type: none"> • The Organization reported than in two separate incidents, two financial advisors gave remote access to their computers to an unknown party who phoned them posing as IT support staff. As a result, personal information stored locally on the computers may have been exposed to unauthorized individuals. • The first incident occurred July 24th, 2014, and the second on August 1st 2014.
Affected individuals	The incident affected 164 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Offered free subscription to credit monitoring service. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta. • Reported the incident to the Office of the Information and Privacy Commissioner of British Columbia and Office of the Privacy Commissioner of Canada.
Steps taken to notify individuals of the incident	Notification sent by mail on August 25, 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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.</p>	<p>The Organization reported that the information might be used for identity theft and fraud, and noted that “the potential harm that could result from the breaches is significant due to the circumstances of the incidents.”</p> <p>In my view, the personal information involved in this incident could be used to cause the harms of identity theft and fraud. These are significant harms.</p>
<p>Real Risk The likelihood that the significant harm 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.</p>	<p>The Organization reported that the incident resulted from malicious intent, and the unauthorized individuals could have obtained access to client information stored locally on laptops; however, the Organization has no way to verify if there was actual access. The unauthorized access continued for 30 minutes in the first incident, and for 2-3 minutes in the second.</p> <p>In my view, the deliberate actions of the callers to obtain unauthorized remote access to computer systems increase the likelihood of harm resulting from this incident.</p>

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. The incident involved sensitive identity information which could be used to cause the significant harms of identity theft and fraud. In particular, the deliberate actions of the callers to obtain unauthorized remote access to the Organization's computer systems increase the likelihood of harm resulting from this incident.

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

I understand the Organization notified the affected individuals by letter dated August 25, 2014, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner