



**PERSONAL INFORMATION PROTECTION ACT  
Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	Sun Life Assurance Company of Canada (Organization)
<b>Decision number (file number)</b>	P2019-ND-056 (File #008903)
<b>Date notice received by OIPC</b>	June 7, 2018
<b>Date Organization last provided information</b>	June 7, 2018
<b>Date of decision</b>	May 6, 2019
<b>Summary of decision</b>	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).
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA “organization”</b>	The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• address,</li><li>• email address,</li><li>• date of birth,</li><li>• medical and dental claim history, and</li><li>• banking information.</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
<b>Description of incident</b>	<ul style="list-style-type: none"><li>• On May 29, 2018, due to an administrative error, a group plan member was able to access another group member’s personal information by logging into the Organization’s mobile app or the secure member website.</li></ul>

	<ul style="list-style-type: none"> <li>• A member reported the incident to the Organization.</li> <li>• The error occurred when assigning the group benefits plan member identification number.</li> <li>• The incident affected 45 members; of these, 7 members had accessed the secure site on May 29, 2018.</li> </ul>
<b>Affected individuals</b>	The incident affected seven (7) individuals residing in Alberta
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Suspended the website and mobile account access.</li> <li>• Notified affected plan members.</li> <li>• Offered a pre-paid, 12-month subscription to a credit monitoring service.</li> <li>• Provided feedback to the employee who caused the incident.</li> <li>• Reviewed the process and supporting documentation with senior managers to strengthen preventative measures.</li> <li>• Re-trained employees.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified by letter on June 6, 2018.
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<p><b>Harm</b> Some damage or detriment or injury that could be caused to 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 type of harm that might result from the incident included “Identity theft/fraud; humiliation/embarrassment”.</p> <p>I agree with the Organization’s assessment. The contact, identity, financial and medical/health information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. These are significant harms.</p>
<p><b>Real Risk</b> 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 affected individuals are employed by the same employer and located in the same city. Where sensitive information was accessed there is a risk of humiliation I embarrassment. While the risk of identify [sic] theft / fraud is unlikely in this context, the potential exists due to the type of information available under a group benefits plan member's web account”.</p>

	<p>In my view, a reasonable person would consider there is a real risk of significant harm in this case, despite the fact the incident did not result from malicious intent. The Organization did not receive confirmation that the information at issue was not further distributed or copied and there may be personal or professional relationships between the affected individuals and those who had access to the information, increasing the likelihood of hurt, humiliation or embarrassment.</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 contact, identity, financial and medical/health information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. These are significant harms. Despite the fact the incident did not result from malicious intent, the Organization did not receive confirmation that the information at issue was not further distributed or copied and there may be personal or professional relationships between the affected individuals and those who had access to the information, increasing the likelihood of hurt, humiliation or embarrassment.

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

I understand the Organization notified affected individuals in a letter dated June 6, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner