



**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>File number</b>	P2017-ND-29 (File #002032)
<b>Date notice received by OIPC</b>	December 18, 2015
<b>Date Organization last provided information</b>	December 18, 2015
<b>Date of decision</b>	February 2, 2017
<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 the 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)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The following information was involved in this incident:</p> <ul style="list-style-type: none"><li>• name,</li><li>• address,</li><li>• policy reference number,</li><li>• investment fund rate,</li><li>• principal amount, and</li><li>• maturity value.</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. Some of the information was collected in Alberta from residents of Alberta.</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 October 14, 2015, the Organization mailed investment confirmation notices to 49 clients.</li> <li>• Between October 19 and October 29, 2015, the Organization received reports from five (5) clients advising that they received investment notices belonging to other clients, along with their own.</li> <li>• The Organization investigated and found that the incident was the result of human error.</li> <li>• The Organization contacted the 5 unintended recipients that reported the incident. Four (4) of the 5 returned the notices they received in error to the Organization.</li> <li>• The 5<sup>th</sup> unintended recipient stated he would forward the investment notices to all three (3) clients whose mail he received in error. One of the three clients reported receiving this communication from the unintended recipient.</li> </ul>
<b>Affected individuals</b>	The incident affected 44 individuals, including 6 residents of Alberta.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Investigated the incident and followed up with the 5 unintended recipients that reported the incident to the Organization.</li> <li>• Notified affected individuals.</li> <li>• Reported the incident to the federal Privacy Commissioner, as well as privacy commissioners in British Columbia, Alberta and Quebec.</li> <li>• Offered complimentary credit monitoring to affected individuals.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	The Organization notified affected individuals in writing between November 2 and November 25, 2015.
<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 “If the information were to fall into the wrong hands, there is risk of financial fraud. For example, an attempt could be made to withdraw a client’s investment funds...”.</p> <p>I accept the Organization’s assessment that the personal information at issue could be used to cause financial fraud. This is a significant harm.</p>

<p><b>Real Risk</b></p> <p>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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident.</p> <p>In my view, there is a real risk of significant harm. Although the incident resulted from human error and not malicious intent, the Organization has reported that at least one of the unintended recipients did not return the information to the Organization and instead forwarded it to affected individuals. It appears that this was done to draw the affected individuals' attention to the incident; nonetheless, the information has not been recovered by the Organization and remains exposed.</p>
<p><b>DECISION UNDER SECTION 37.1(1) OF PIPA</b></p>	
<p>Given the information reported by the Organization, I have concluded that there is a real risk of harm to the affected individuals in this case. I accept the Organization's assessment that the personal information at issue could be used to cause the significant harm of financial fraud. Although the incident resulted from human error and not malicious intent, the Organization has reported that at least one of the unintended recipients did not return the information to the Organization and instead forwarded it to affected individuals. It appears that this was done to draw the affected individuals' attention to the incident; nonetheless, the information has not been recovered by the Organization and remains exposed.</p> <p>I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization notified the affected individuals in writing between November 2 and November 25, 2015. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton  
Information and Privacy Commissioner