



**PERSONAL INFORMATION PROTECTION ACT  
Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	AIG Insurance Company of Canada (Organization)
<b>Decision number (file number)</b>	P2021-ND-335 (File #022387)
<b>Date notice received by OIPC</b>	July 22, 2021
<b>Date Organization last provided information</b>	December 16, 2021
<b>Date of decision</b>	March 10, 2022
<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 whose personal information was collected in Alberta pursuant to section 37.1 of <i>the 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>• home address,</li><li>• medical diagnoses,</li><li>• description of medical conditions, and</li><li>• social insurance number.</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.</p>
<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

<p><b>Description of incident</b></p>	<ul style="list-style-type: none"> <li>On or about September 26, 2020, the Organization was notified by one of its third party claims processors - Arthur J. Gallagher / Gallagher Bassett (collectively, Gallagher) - that Gallagher was the subject of a ransomware attack. “[An] unknown individual accessed or acquired data” from Gallagher’s network between June 3 and September 26, 2020.</li> <li>Initially, the third party reported that data under the control of the Organization was not impacted in the incident. However, “Upon further analysis, Gallagher subsequently informed [the Organization] that personal information relating to certain Canadian claimants was impacted by this incident”.</li> </ul>
<p><b>Affected individuals</b></p>	<p>The incident affected 49 individuals whose information was collected in Alberta.</p>
<p><b>Steps taken to reduce risk of harm to individuals</b></p>	<ul style="list-style-type: none"> <li>“[The Organization] is working with Gallagher to ensure the notifications to the individuals are provided accurately to all impacted individuals and as quickly as feasibly possible.”</li> <li>Received information from Gallagher about the steps taken by the claims administrator to enhance technical and administrative safeguards.</li> <li>Conducted an internal security investigation and confirmed that the Organization’s internal systems were not affected in the incident.</li> </ul>
<p><b>Steps taken to notify individuals of the incident</b></p>	<p>Affected individuals were notified in writing by the Organization’s third party. Notifications began on July 30, 2021, and completed in September 2021.</p>
<p><b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b></p>	
<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 did not report the possible harm(s) that could be caused to affected individuals as a result of the incident. On December 16, 2021, the Organization said:</p> <p style="text-align: center;"><i>There was no direct impact to [the Organization’s] IT systems or operations. However, [the Organization] has considered the potential for harm to the information of individuals impacted based on the combination of information that may have been exposed for individual associated with ... claims.</i></p> <p>In my view, a reasonable person would consider that the contact, identity (social insurance number), and claims (medical diagnoses, description of medical conditions) information at issue could be used to cause the harms of identity theft, or embarrassment, hurt and humiliation. These are significant harms.</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>On December 16, 2021, the Organization reported that its...</p> <p><i>... assessment of the likelihood of harm is low. Gallagher has confirmed that they have no evidence of any actual or attempted misuse of information and have no indication the information is in the possession or control of an unauthorized person or party. Nevertheless, credit monitoring has been offered to all individuals as an additional protective measure.</i></p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (ransomware). The lack of reported misuse does not mitigate against future harm as identity theft, embarrassment, hurt or humiliation may occur months or years after a breach. Further, the unknown actor had access to the Organization's service provider's network for approximately four months.</p>
<p><b>DECISION UNDER SECTION 37.1(1) OF PIPA</b></p>	
<p>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.</p> <p>A reasonable person would consider that the contact, identity (social insurance number), and claims (medical diagnoses, description of medical conditions) information at issue could be used to cause the harms of identity theft, or embarrassment, hurt and humiliation. These are significant harms.</p> <p>The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (ransomware). The lack of reported misuse does not mitigate against future harm as identity theft, embarrassment, hurt or humiliation may occur months or years after a breach. Further, the unknown actor had access to the Organization's service provider's network for approximately four months.</p> <p>I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization's third party notified affected individuals in writing between July 30, 2021 and September 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton  
Information and Privacy Commissioner