



**PERSONAL INFORMATION PROTECTION ACT**  
**Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	Investors Group (Organization)
<b>Decision number (file number)</b>	P2018-ND-053 (File #008485)
<b>Date notice received by OIPC</b>	April 26, 2018
<b>Date Organization last provided information</b>	April 26, 2018
<b>Date of decision</b>	May 7, 2018
<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 copies of client applications, void cheques and personal financial reviews containing the following information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• address,</li><li>• social insurance number, and</li><li>• financial information.</li></ul> <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>
<b>DESCRIPTION OF INCIDENT</b>	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
<b>Description of incident</b>	<ul style="list-style-type: none"><li>• During the afternoon of April 8, 2018, a vehicle belonging to one of the Organization’s financial advisors was broken into. A brief case containing a laptop computer and 5 client files was stolen.</li></ul>

	<ul style="list-style-type: none"> <li>• The incident was discovered on April 9, 2018.</li> <li>• The laptop was encrypted and had strong password protection.</li> <li>• The Organization did not report recovering the client files.</li> </ul>
<b>Affected individuals</b>	The incident affected five (5) clients.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Offered affected individuals reimbursement for credit monitoring services.</li> <li>• Tagged affected individuals' accounts with confidentiality alerts.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified by letter on or about April 16, 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 "One potentially [sic] type of harm that could result is identity theft for the clients whose personal information was stolen in paper format from the client file. The laptop itself however was protected by encryption and strong password requirements so we don't consider this to be a potential harm".</p> <p>In my view, the contact and identity information in the paper documents, along with the financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.</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 "We do not consider it likely that harm will result. This is because the target of the theft was the contents of the vehicle. Although we are only guessing at their motive(s), the Consultant did report the incident to the authorities and during this process was informed by the authorities that the crime was a random event. We also don't consider it likely that harm will result because this appears to be a random event."</p> <p>In my view, the likelihood of harm resulting from this incident is increased as the breach was a result of malicious intent (vehicle break-in and theft). The Organization did not report recovering the paper client files. The Organization can only speculate as to the motive of the thief.</p>
<b>DECISION UNDER SECTION 37.1(1) OF PIPA</b>	
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 and identity information in the paper documents, along with the financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased as the breach was a result of malicious intent (vehicle break-in and theft). The Organization did not report recovering the paper client files. The Organization can only speculate as to the motive of the thief.

I require the Organization to notify the affected individuals in Alberta, whose information was included in the paper documents, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that affected individuals were notified by letter on or about April 16, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner