



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

<b>Organization providing notice under section 34.1 of PIPA</b>	World Financial Group Canada Inc. (Organization)
<b>Decision number (file number)</b>	P2021-ND-171 (File #017955)
<b>Date notice received by OIPC</b>	April 15, 2020
<b>Date Organization last provided information</b>	June 22, 2021
<b>Date of decision</b>	August 27, 2021
<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) 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>• date of birth,</li><li>• address,</li><li>• social insurance number,</li><li>• banking information,</li><li>• photo ID,</li><li>• financial information,</li><li>• medical/health information, and</li><li>• account information.</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 information was collected in Alberta, PIPA applies.</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>• On or about April 6, 2020, an advisor with the Organization had their vehicle stolen from their driveway.</li> <li>• In the vehicle was a workbag with a password-protected laptop containing client information.</li> <li>• The advisor's spouse discovered that the vehicle was missing on their way to work.</li> </ul>
<b>Affected individuals</b>	The incident affected 74 individuals, including three (3) individuals who had their information collected in Alberta.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Escalated the incident to the Privacy Officer.</li> <li>• Notified insurance providers and fund companies in order to heighten the security precautions for the affected clients.</li> <li>• Reminding staff and advisors of the importance of being diligent in keeping belongings containing client information safe to help prevent future breaches.</li> <li>• Notified the local police of the theft.</li> <li>• Offered affected individuals credit monitoring services as a cautionary step to help mitigate against fraud risks.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	The affected individuals were notified by letter sent by email on May 12, 2020.
<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 the possible harms that may occur as a result of the breach are:</p> <ul style="list-style-type: none"> <li>- <i>Identity Fraud</i></li> <li>- <i>Account Take Over</i></li> <li>- <i>Funds Re-Directed to a Third Party</i></li> </ul> <p>In my view, a reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the harms of identity theft and fraud. Medical/health information could be used to cause hurt, humiliation and embarrassment. These are all 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,</p> <p><i>The likelihood of harm that will result in this event is of medium impact because the advisor believes that the theft occurred with the intention to resell the vehicle and its contents for money no interest in the information on the laptop. However, given the type of information that was on the laptop in itself (sic), if the intent was to obtain personal information and use it for fraudulent purposes then the likelihood of harm is high.</i></p>

	<p>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the breach is the result of malicious intent (vehicle break-in and theft). The Organization did not report that the laptop was encrypted or recovered, and can only speculate as to the motives of the thief.</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, and financial information at issue could be used to cause the harms of identity theft and fraud. Medical/health information could be used to cause hurt, humiliation and embarrassment. These are all significant harms. The likelihood of harm resulting from this incident is increased because the breach is the result of malicious intent (vehicle break-in and theft). The Organization did not report that the laptop was encrypted or recovered, and can only speculate as to the motives of the thief.</p> <p>I require the Organization to notify the affected individuals in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the affected individuals were notified by letter sent by email on May 12, 2020 in accordance with the Regulation. The Organization is not required to notify the individuals again.</p>	

Jill Clayton  
Information and Privacy Commissioner