



**PERSONAL INFORMATION PROTECTION ACT  
Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	World Financial Group Insurance Agency of Canada Inc. (Organization)
<b>Decision number (file number)</b>	P2020-ND-162 (File #016766)
<b>Date notice received by OIPC</b>	March 27, 2020
<b>Date Organization last provided information</b>	October 28, 2020
<b>Date of decision</b>	November 24, 2020
<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>• date of birth,</li><li>• mailing address,</li><li>• Social Insurance Number,</li><li>• photo identification,</li><li>• financial information,</li><li>• 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 this 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	

<p><b>Description of incident</b></p>	<ul style="list-style-type: none"> <li>On March 1, 2020, a vehicle belonging to an employee of the Organization was broken into. A password protected laptop containing client information and a locked bag of client files were stolen from the vehicle.</li> <li>Law enforcement was notified on the same day, followed by notification to the Organization’s privacy personnel on March 6, 2020.</li> </ul>
<p><b>Affected individuals</b></p>	<p>The incident affected 41 individuals, of which 31 are residents of Alberta.</p>
<p><b>Steps taken to reduce risk of harm to individuals</b></p>	<ul style="list-style-type: none"> <li>Reported incident to law enforcement.</li> <li>Notified insurance providers.</li> <li>Sending letters to affected clients.</li> <li>Reiterated the importance of being diligent and ensuring belongings containing client information are kept safe.</li> <li>Advised agents to not save sensitive information to personal devices and ensure client files are locked away in branch offices.</li> </ul>
<p><b>Steps taken to notify individuals of the incident</b></p>	<p>Affected individuals were notified by telephone, in-person, or email by April 8, 2020.</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 reported the possible harms that might result from this incident as follows:</p> <ul style="list-style-type: none"> <li>“Identity Fraud”</li> <li>“Account Take Over”</li> <li>“Funds Re-Directed to a Third Party”</li> </ul> <p>In my view, a reasonable person would consider that the identity, contact, and financial information at issue could be used to cause the harms of identity theft, financial loss, and fraud. Financial and health information could also be used to cause the harms of humiliation, embarrassment, and damage to reputation. 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. The theft of the laptop and client files likely occurred as the perpetrator was looking for items of value which can be resold for money. However, given the sensitive nature of the information that was on the laptop and the personal information that may be in the client files, if the intent was to obtain personal information and</i></p>

	<p><i>use it for fraudulent purposes then the likelihood of harm is high.</i></p> <p>In my view, the likelihood of harm resulting from the incident is increased because the personal information was compromised due to the malicious action of an unknown third party (vehicle break-in, theft). Further, the Organization did not report recovering the records, nor did they indicate whether the laptop was encrypted, increasing the risk of unauthorized access.</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.

A reasonable person would consider that the identity, contact, and financial information at issue could be used to cause the harms of identity theft, financial loss, and fraud. Financial and health information could also be used to cause the harms of humiliation, embarrassment, and damage to reputation. These are all significant harms.

The likelihood of harm resulting from the incident is increased because the personal information was compromised due to the malicious action of an unknown third party (vehicle break-in, theft). Further, the Organization did not report recovering the records, nor did they indicate whether the laptop was encrypted, increasing the risk of unauthorized access.

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

I understand the Organization notified affected individuals by telephone, in-person, or email by April 8, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner