



**PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision**

Organization providing notice under section 34.1 of PIPA	ivari (Organization)
Decision number (file number)	P2020-ND-168 (File #016771)
Date notice received by OIPC	March 24, 2020
Date Organization last provided information	October 14, 2020
Date of decision	December 1, 2020
Summary of decision	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).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• physical address,• driver’s license,• permanent resident card,• social insurance number,• date of birth, and• financial information. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.</p>
DESCRIPTION OF INCIDENT	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

Description of incident	On March 1, 2020, a password protected laptop, and a bag containing client files, were stolen from a locked vehicle (break-in). Local police authorities were informed on the same day.
Affected individuals	The incident affected 7 individuals, of whom 6 had their personal information collected in Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Employee changed their passwords to advisor portals. • The Organization reminded the advisor that they should not keep client information on their laptop.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter between March 13 and April 8, 2020.

REAL RISK OF SIGNIFICANT HARM ANALYSIS

Harm 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>The Organization reported the possible harm that might result is “Identity theft”.</p> <p>In my view, a reasonable person would consider that the contact, identity, and financial information at issue could be used for the purposes of identity theft, fraud, and financial loss. These are significant harms.</p>
Real Risk 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>The Organization reported that its “...best assessment is that there is a moderate risk to the client’s [sic].”</p> <p>In my view, the likelihood of harm resulting from this incident is increased as the personal information was compromised due to the malicious action of an unknown third party (vehicle break-in, theft). The Organization did not report recovering the document or the laptop. Further, while the Organization affirmed the laptop was password protected, it did not clearly indicate that data on the device was encrypted.</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 contact, identity, and financial information at issue could be used for the purposes of identity theft, fraud, and financial loss. These are significant harms.

The likelihood of harm resulting from this incident is increased as the personal information was compromised due to the malicious action of an unknown third party (vehicle break-in, theft). The Organization did not report recovering the document or the laptop. Further, while the Organization

affirmed the laptop was password protected, it did not clearly indicate that data on the device was encrypted.

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 letter between March 13 and 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