



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	ivari (Organization)
Decision number (file number)	P2021-ND-036 (File #016774)
Date notice received by OIPC	March 11, 2020
Date Organization last provided information	November 5, 2020
Date of decision	February 23, 2021
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">• images of identification documents (driver’s license, provincial identification card, passport, permanent resident card), and• insurance policy statements (including name, address, date of birth, name of beneficiary, value of policy) <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>
DESCRIPTION OF INCIDENT	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On February 28, 2020, an insurance advisor’s vehicle was broken into. A briefcase containing two laptops and client paper files was stolen.

	<ul style="list-style-type: none"> • The incident was discovered and reported to local police authorities on the same day. • It is reported that one of the laptops was not password protected, and neither device was confirmed to be encrypted.
Affected individuals	The incident affected 61 individuals who had their personal information collected in Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Reported the theft to local police on February 28, 2020. • Reported the breach to the Office of the Privacy Commissioner of Canada on March 11, 2020. • Changed passwords for portals used by the advisor to access client information. • Privacy officer sent an email to all advisors, re-emphasizing the importance of protection of client information.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing between March 11 and 13, 2020.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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>	<p>The Organization reported the possible harm that might result from the incident include “financial loss, identity theft, and negative effects on the credit record”.</p> <p>I agree with the Organization’s assessment. A reasonable person would consider the contact, identity and insurance information at issue could be used to cause the harms of identity theft and fraud. Beneficiary and policy value information could also be used to cause the harms of hurt, humiliation, and damage to relationships. These are significant harms.</p>
<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>	<p>The Organization reported that “the likelihood of harm would be moderate”.</p> <p>In my view, a reasonable person would consider 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 (vehicle break-in, theft). Further, one of the laptops was not password protected and the organization did not confirm that either device was encrypted, increasing the likelihood that personal information could be accessed without authorization. The organization did not report recovering the devices or records.</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 the contact, identity and insurance information at issue could be used to cause the harms of identity theft and fraud. Beneficiary and policy value information could also be used to cause the harms of hurt, humiliation, and damage to relationships. These are significant harms.

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 (vehicle break-in, theft). Further, one of the laptops was not password protected and the organization did not confirm that either device was encrypted, increasing the likelihood that personal information could be accessed without authorization. The organization did not report recovering the devices or records.

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 in writing between March 11 and 13, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner