Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	ivari (Organization)
Decision number (file number)	P2021-ND-265 (File #020717)
Date notice received by OIPC	April 21, 2021
Date Organization last provided information	April 21, 2021
Date of decision	February 9, 2022
Summary of decision	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 *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • telephone number, • email address, • date of birth, and • country of birth. For one individual, the following information is also at issue: • driver license number, • answers to medical, health and personal history questions. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On April 12, 2021, an insurance advisor saw a blinking message on her computer screen. The message appeared to be from "Microsoft" and provided a number to call. • The advisor called the number and followed instructions to download an "Ultraview", which allowed an unauthorized party to gain control of her computer. • The unauthorized party indicated the advisor's email and online banking were hacked, and asked for the toll free number on the back of her credit card. When the advisor refused to provide it, she noticed files on her desktop disappearing and she quickly turned off her computer and hung up the phone. • The files that were removed contained personal information of her insurance clients.
Affected individuals	The incident affected four (4) individuals.
Steps taken to reduce risk of harm to individuals	• Changed passwords used to access client information. • Placed a note on client files to complete extra authentication. • Contacted IT department. • Updated ant-virus software done by the IT.
Steps taken to notify individuals of the incident	The affected individuals were notified by text message on April 12, 2021 and by formal letter on April 21, 2021.
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.	The Organization reported the possible harms that may occur as a result of the breach are "financial loss, identity theft, humiliation, damage to relationships, and negative effect on credit record." I agree with the Organization's assessment. A reasonable person would consider that the contact and identity information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. Medical information could be used to cause hurt, humiliation and embarrassment. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.
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.	The Organization reported, *The personal information was compromised due to malicious action of an unknown third party so the likelihood is high.* I agree with the Organization's assessment. A reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach is the result of malicious intent

	(deliberate action, impersonation) and it appears that the information is still in the possession of the perpetrator.

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 and identity information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. Medical information could be used to cause hurt, humiliation and embarrassment. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased as it is the result of malicious intent (deliberate action, impersonation) and it appears that the information is still in the possession of the perpetrator.

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 the affected individuals by text message on April 12, 2021 and by formal letter on April 21, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner