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	Travel Healthcare Insurance Solutions Inc. o/a guard.me International Insurance (Organization)
Decision number (file number)	P2021-ND-281 (File #022175)
Date notice received by OIPC	July 12, 2021
Date Organization last provided information	January 5, 2022
Date of decision	February 21, 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 those individuals whose personal information was collected in Alberta pursuant to section 37.1 of *the Personal Information Protection Act* (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"	The incident involved all or some of the following information:
	• name,
	• surname,
	• date of birth,
	• "contact details" including email address,
	• hashed passport number,
	• hashed password,
	• employee ID,
	• bank and financial information,
	• health information such as:
	  ○ diagnosis,
	  ○ treatment type,
	  ○ prescription information,
	  ○ location,
	  ○ service,
	  ○ doctor's name,
	  ○ billing information,
	  ○ claim information, and
	  ○ claim adjuster's notes.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	On or about June 19, 2021, the Organization was subject to an SQL injection attack. The attacker compromised two SQL databases; records were deleted and a ransom note was inserted.
Affected individuals	The incident affected 1,280,866 individuals, including 389 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Obtained "confirmation that the data was destroyed" from the attacker and "prevent[ed] the data from being released." • Offered credit monitoring services to affected individuals. • Consulted with an IT security firm to review infrastructure and provide recommendations. • Implemented a number of IT security enhancements including resetting passwords and enabling multi-factor authentication. • Hiring a security analyst / dedicated internal security resource.
Steps taken to notify individuals of the incident	The Organization reported that affected individuals "will likely be notified by July 16, 2021" via "Mail, e-mail, or through educational institutions." On December 17, 2021, the Organization reported that "notifications were delivered by e-mail where [the Organization] had contact information for those affected individuals. Additionally, educational institutions also delivered notifications to affected individuals" and also "Notifications were provided … over the course of the period of July 16, 2021 to September 17, 2021." On January 5, 2022, the Organization clarified that for some affected individuals, no contact information was available. Instead, those individuals were notified indirectly via their educational institution and a public notice published on the Organization's website. "The rationale for the indirect notification was the lack of contact information."

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 of "Identifity [sic.] theft; fraud." I accept the Organization's assessment. A reasonable person would consider the identity (date of birth), employment (employee ID), financial (banking), and health information could be used to cause the harms of identity theft and fraud. Health information could be used to cause the harms of hurt, humiliation or embarrassment. Email addresses could be used for the purposes of phishing, increasing the affected individuals' 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 that "There is a medium risk of identity theft or fraud." The Organization's draft notice for affected individuals also said that they "have no reason to believe there was any actual or attempted misuse of your personal information". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, possible exfiltration of records, and ransom demand). The lack of reported misuse of the personal information does not mitigate against future harms as identity theft, fraud, and phishing can occur months or years after a breach. Further, while the Organization obtained assurances from the threat actor that the data were destroyed, it is unclear whether the assurances are reliable.

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 identity (date of birth), employment (employee ID), financial (banking), and health information could be used to cause the harms of identity theft and fraud. Health information could be used to cause the harms of hurt, humiliation or embarrassment. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, possible exfiltration of records, and ransom demand). The lack of reported misuse of the personal information does not mitigate against future harms as identity theft, fraud, and phishing can occur months or years after a breach. Further, while the Organization obtained assurances from the threat actor that the data were destroyed, it is unclear whether the assurances are reliable.

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 some affected individuals by email between July 16, 2021 and September 17, 2021, in accordance with the Regulation. However, I also understand that the Organization lacked direct contact information for some affected individuals. In those cases, affected individuals were notified indirectly via their educational institution and a public notice published on the Organization's website.

Section 19.1(2) of the Regulation states that "notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

Given the Organization's submission, I accept that indirect notice as described by the Organization is reasonable where the Organization is unable to contact the affected individuals directly.

The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner