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	AVENIR GLOBAL Inc. (Organization)
Decision number (file number)	P2021-ND-308 (File #022008)
Date notice received by OIPC	June 30, 2021
Date Organization last provided information	December 19, 2021
Date of decision	March 4, 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 a holding and management company of communications firms. 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, • civic address, • email address, • banking information, • driver's license, • social insurance number, and • medical information such as medical condition of individuals. The Organization reported, "information in the hands of the Company is information on employees or information shared by corporate clients or individuals for specific mandate." 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.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On December 29, 2020, the Organization was informed that it was the target of a ransomware attack, which affected its systems in a number of jurisdictions. • Some information shared with the Organization or one of its subsidiaries was consequently compromised. • The Organization's investigation suggests the breach likely resulted from a phishing email. • The Organization does not have any information to suggest that the accessed information has been misused. • The Organization reported, "to the contrary, we have taken stringent measures to ensure that the compromised data were not copied and disclosed and are no longer accessible to the unauthorized third party."
Affected individuals	The incident affected 3,493 individuals, which includes 19 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported numerous steps taken to improve IT security and reduce the risk of similar cyber attacks.
Steps taken to notify individuals of the incident	Affected employees were notified by letter from January 26, 2021 to July 29, 2021. Affected individuals, who shared personal information with a client of the Organization, were notified by letter or email on August 5, 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, "Information could potentially be used for identity theft." In my view, a reasonable person would consider the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Medical information could be used to cause embarrassment and humiliation. 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, *A misuse of the information is unlikely to happen at this point as the breach occurred from November 17th, to December 29th 2020 and the unauthorized user confirmed deletion of the data. To date, no employee has reported a misuse of their information.* In my view, 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 (deliberate intrusion, ransom demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Although the Organization reported that, the unauthorized third party "...is a known hacker which has the reputation of being "reliable" if the ransom is paid" I do not find this to be reassuring. The Organization can only speculate as to the motives and intentions 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 the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Medical information could be used to cause embarrassment and humiliation. 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 an unknown third party (deliberate intrusion, ransom demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Although the Organization reported that, the unauthorized third party "...is a known hacker which has the reputation of being "reliable" if the ransom is paid" I do not find this to be reassuring. The Organization can only speculate as to the motives and intentions 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 affected individuals by letter between January 26, 2021 and July 29, 2021, and on August 5, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner