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	TAM International Inc. (Organization)
Decision number (file number)	P2021-ND-267 (File #019293)
Date notice received by OIPC	February 4, 2021
Date Organization last provided information	October 27, 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 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's head office is located in Houston, Texas, USA. 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 all or some of the following information: • name, • address, • social insurance number, • date of birth, and • other information collected in the ordinary course of the individual's employment. 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 or about Saturday, October 24, 2020, cyber criminals encrypted some of the Organization's servers and network-connected computers and demanded a ransom to decrypt them. They also claimed that they had stolen files from the Organization's servers, targeting some of the executive team. • The Organization's investigation discovered that the attack originated from a company laptop for an employee based outside of the United States. • The laptop was compromised via a phishing email in March 2020, and the criminals loaded malware onto the laptop, which later spread to the Organization's network. • Because of limited available log data, the Organization was unable to determine whether the criminals actually acquired, or the extent to which they accessed, sensitive personal information for its non-executive employees. • The criminals claimed to have taken copies of certain server files, but the Organization's investigation was only able to confirm that the personal data of some of its executives were actually copied. • The incident ended on October 24, 2020.
Affected individuals	The incident affected 47 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Reset passwords to network accounts and implemented additional security controls to prevent further unauthorized access to the network. • Notified law enforcement. • Retained cybersecurity forensic experts to investigate the incident, restore IT services, and help safely and securely resume operations. • Implemented additional endpoint security and actively monitored threat intelligence solutions to protect servers and network connected devices from re-infection. • Implemented methods that limit the amount of traffic to, from, and across the network, and will adopt additional measures to train and inform employees of cyber risks.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter or email on January 29, 2021. The Organization also posted a temporary website notice.

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 were "Unknown". In my view, a reasonable person would consider the contact, identity and employment information could be used to cause the significant harms of identity theft, fraud and/or financial loss.
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 the likelihood that significant harm will result is "Unknown." In its notification to affected individuals, the Organization stated, "We are unaware of any misuse of any employee information at this time." 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 (deliberate intrusion, ransom demand), and the laptop may have been compromised for approximately 7 months. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft, fraud and/or financial loss can occur months and even years after a data breach. Finally, the personal information at issue was accessed and copied by the unknown third party.

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 employment information could be used to cause the significant harms of identity theft, fraud and/or financial loss.

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), and the laptop may have been compromised for approximately 7 months. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft, fraud and/or financial loss can occur months and even years after a data breach. Finally, the personal information at issue was accessed and copied by the unknown third party.

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 or email on January 29, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner