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	Premier Tech Limited (Organization)
Decision number (file number)	P2021-ND-300 (File #020334)
Date notice received by OIPC	March 26, 2021
Date Organization last provided information	March 26, 2021
Date of decision	March 3, 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, • job type, • job title, • hours worked, • gross pay, and • deductions. 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 January 25, 2021, the Organization discovered that it was the victim of a cybersecurity attack by an unauthorized third party. The malicious actor deployed ransomware to encrypt the Organization's technology infrastructure and to exfiltrate data. • On February 11, 2021, the Organization discovered that the unauthorized third party may have gained access to and may have exfiltrated the personal information of its team members and immediately undertook an additional investigation to determine the scope of the information affected. • The incident occurred between January 13, 2021 and January 25, 2021.
Affected individuals	The incident affected 2,484 Canadians, including 121 in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged a cyber forensic firm to investigate, determine how the security incident occurred, the scope, and to assist with remediation efforts. • Offered identity theft and credit monitoring services to potentially affected individuals for a period of 24 months. • Tightened internal processes concerning the operations of the IT infrastructure. • Notified the Surete du Québec.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or letter mail on March 26, 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 its assessment "… that there is a risk of hurt, humiliation and embarrassment since the potential personal information involved in the incident is employment information." In my view, a reasonable person would consider the contact and employment information at issue could be used to cause the significant harms of hurt, humiliation and embarrassment, and possibly identity theft and fraud.
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 it is … *… of the view that the likelihood that harm could result is low to moderate. While [the Organization] has no evidence confirming that the personal information at issue has been compromised or misused by the external actor, the personal information involved in the incident is nonetheless sensitive and could be used for the purposes identified above. The fact that the incident was caused as a result of the actions of an unknown*

	actor with malicious intent additionally increases the likelihood that harm could result. 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 information was exposed for almost 2 weeks. Although the Organization reported that it "has no evidence confirming that the personal information at issue has been compromised or misused by the external actor", this is not a mitigating factor as identity theft, fraud, embarrassment and humiliation can happen months and even years after a data breach.

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 and employment information at issue could be used to cause the significant harms of hurt, humiliation and embarrassment, and possibly identity theft and fraud.

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 information was exposed for almost 2 weeks. Although the Organization reported that it "has no evidence confirming that the personal information at issue has been compromised or misused by the external actor", this is not a mitigating factor as identity theft, fraud, embarrassment and humiliation can happen months and even years after a data breach.

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 email or letter mail on March 26, 2021. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner