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	Westech Industrial Ltd. (Organization)
Decision number (file number)	P2021-ND-242 (File #019777)
Date notice received by OIPC	February 26, 2021
Date Organization last provided information	July 28, 2021
Date of decision	November 30, 2021
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 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, • date of birth, • social insurance number, • mailing address, • emergency contacts, • extended medical information, • compensation, and • performance reviews. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On February 10, 2021, the Organization detected suspicious network activity on its servers. The following day, February 11, 2021, the Organization received a ransom demand via email. • The Organization reports that although deployment of ransomware was threatened, no malicious files were found nor were files encrypted. • No root cause of the breach was identified.
Affected individuals	The incident affected 85 of individuals, including 30 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified police. • Recommended that affected individuals monitor their credit report and offered credit monitoring services. • Recommended that affected individuals change their passwords. • Engaged a cyber security firm to conduct a review. • Rebuilt network. • Remediated vulnerabilities. • Enabled additional authentication controls. • Enhanced monitoring of network. • Implementing a cyber-awareness training program.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on February 11, 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 "It is possible that sufficient data would exist to attempt identity theft." In my view, a reasonable person would consider the contact, identity (social insurance number), extended medical information, and employment information at issue could be used to cause the harms of identity theft and fraud. Extended medical information and employment information (performance reviews and compensation) could also be used in combination with the above to cause the harms of embarrassment, hurt or humiliation, damage to reputation or relationships, and loss of business or professional opportunities. These are 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	The Organization reported that the likelihood of harm is "Unknown, but unlikely since it does not reside in a consolidated form." Additionally, "To date we have seen no evidence of this information being in anyones [sic] hands, however, we did disclose

between the incident and the possible harm.	the breach to affected parties and offered them credit monitoring services." Despite the above, the Organization's notification letter states: "While we do not know what was taken from us, a breach of our network does include the potential to access personnel information. Personnel information is stored in a locked and access restricted environment, but in the context of a network breach there is no assurance that this wasn't obtained." 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 a third party (deliberate intrusion and ransom demand). The Organization could not rule out the possibility that the personal information was accessed by unauthorized parties. Personal information not being "in a consolidated form" does not mitigate against unauthorized access or misuse. Additionally, a lack of evidence that the information has been accessed or misused does not mitigate against future harm; identity theft and fraud can occur months or years after a 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, identity (social insurance number), extended medical information, and employment information at issue could be used to cause the harms of identity theft and fraud. Extended medical information and employment information (performance reviews and compensation) could also be used in combination with the above to cause the harms of embarrassment, hurt or humiliation, damage to reputation or relationships, and loss of business or professional opportunities. These are 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 third party (deliberate intrusion and ransom demand). The Organization could not rule out the possibility that the personal information was accessed by unauthorized parties. Personal information not being "in a consolidated form" does not mitigate against unauthorized access or misuse. Additionally, a lack of evidence that the information has been accessed or misused does not mitigate against future harm; identity theft and fraud can occur months or years after a 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 on February 11, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner