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	Metal-Fab Industries Ltd. (Organization)
Decision number (file number)	P2021-ND-341 (File #019209)
Date notice received by OIPC	January 28, 2021
Date Organization last provided information	August 24, 2021
Date of decision	March 10, 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 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, • email address, • social insurance number, and • banking information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 2, 2021, the Organization discovered that it was the victim of a cyber-attack that encrypted its IT environment. • The breach was discovered the same day during regular on-site maintenance.

	• The Organization reported that the threat actor's main interest was a ransom payment.
Affected individuals	The incident affected 49 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified the RCMP. • Restored systems from backup. • Removed user administrative rights. • Adjusted internal IT practices. • Hardened remote access practices and protocols. • Upgraded anti-virus software. • Offered credit monitoring services to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on January 29, 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: *The potential unauthorized disclosure of the personal information, as well as reputational harm to the organization as a result of a loss of confidence of the employees impacted.* *The above noted personal information was encrypted. We don't know whether it was also "stolen" and used for illegal purposes, such as identity theft.* In my view, a reasonable person would consider that the 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 the above. 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 between the incident and the possible harm.	The Organization reported that harm is "Possible, but not likely." Further, the Organization said: *Our consultants in this matter were of the opinion that it was rather unlikely that the criminals wanted anything more than ransom money, but of course we can't be sure of that. We also provide all our employees with free-of-charge credit monitoring through Equifax and to this point no suspicious activities have been reported to us.* 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 a third party (deliberate intrusion, encryption of files, ransom demand). The Organization does not know if the information was "stolen" and can only speculate as to the motives of the perpetrator. A lack of reported suspicious activity does not mitigate against future harms as 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 that the 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 the above. 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, encryption of files, ransom demand). The Organization does not know if the information was "stolen" and can only speculate as to the motives of the perpetrator. A lack of reported suspicious activity does not mitigate against future harms as 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 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