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	Minerals Technologies Inc. (Organization)
Decision number (file number)	P2021-ND-202 (File #018851)
Date notice received by OIPC	January 4, 2021
Date Organization last provided information	January 4, 2021
Date of decision	October 18, 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 the individual 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, • home address, • mailing address, • telephone number, • social insurance number, • date of birth, • email address, • banking information (account type, routing number, account number), • benefits plan information (policy numbers, beneficiaries), • salary history, and • pay history. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about October 20, 2020, the Organization was victim to a ransomware attack. The incident was discovered when employees found access to their devices was restricted. • On October 22, 2020, the Organization's breach investigation determined that personal information about its current and former employees may have been accessed by the threat actor.
Affected individuals	The incident affected 12,223 individuals, including 1 individual whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Offered affected individual a credit monitoring and identity theft protection service. • Retained an IT firm to investigate the breach, assist in remediation, and implement additional security measures. • Established a security and infrastructure roadmap to improve security of the organization's environment.
Steps taken to notify individuals of the incident	The affected individuals were notified by letter on December 18, 2020.
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 may include identity theft, fraud and financial loss". I agree with the Organization's assessment. A reasonable person would consider the identity, financial, and employment information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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: *While we have no evidence of actual harm to affected individuals, it is possible that the personal information of current and former employees could be misused for identity theft purposes.* *However, we believe the likelihood of harm to be mitigated to the extent affected individuals register for the two-years of credit monitoring and protection that we have offered.*

	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 deployment of ransomware). A lack of evidence of misuse does not mitigate against future harm as identity theft, fraud, or financial loss can occur months or even 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 identity, financial, and employment information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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 deployment of ransomware). A lack of evidence of misuse does not mitigate against future harm as identity theft, fraud, or financial loss can occur months or even years after a breach.

I require the Organization to notify the affected individual 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 the affected individuals by letter on December 18, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner