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	Copper Mountain Mining Corporation (Organization)
Decision number (file number)	P2023-ND-018 (File #028567)
Date notice received by OIPC	January 10, 2023
Date Organization last provided information	January 25, 2023
Date of decision	October 26, 2023
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 some or all of the following information: • name, • address, • date of birth, • email address, • government identification numbers (such as Social Insurance Number), • pay and direct deposit information, and • employee file information. 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 December 27, 2022, the Organization's IT systems at its corporate office were subject to a ransomware attack that encrypted several of its servers and business applications. • The Organization determined that the threat actor likely gained unauthorized access to and likely exfiltrated certain data from its IT systems, including certain personal information.
Affected individuals	The incident affected 1500 individuals, including approximately 50 Albertans.
Steps taken to reduce risk of harm to individuals	The steps taken by the Organization includes but is not limited to the following: • Took action to isolate the impact of the incident • Engaged a leading cybersecurity firm to assist it in securing its systems and to assist counsel in investigating the incident. • Reported the incident to law enforcement • Offered a minimum of one year of credit monitoring and identity theft insurance services. • Listed additional steps recipients can take to help protect themselves. • Continuing to assess the risks associated with the incident and are actively establishing additional safeguards to mitigate further risks. • Forced password resets. • Implemented certain security enhancements. • Provided employees with additional guidance on phishing and related scams.
Steps taken to notify individuals of the incident	The Organization issued a press release and notified current employees and directors by email on December 29, 2022. The Organization sent a follow-up notice by email on January 5, 2023. The Organization notified former employees by email or mail between January 16 and January 19, 2023. The Organization notified former directors by email on January 23, 2023. CMMC has to date been unable to identify contact information for 15 potentially affected former employees.
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	The Organization reported, *Certain groups of potentially affected individuals may be subject to possible harm as a result of this incident including a heightened risk of identity theft, fraud and/or phishing.*

also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	In my view, a reasonable person would consider the contact, identity, and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Employee file information could be used to cause hurt, harm or embarrassment. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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... *The likelihood that harm will result is heightened because the threat actor had malicious intent and had threatened to post exfiltrated information on the "dark web."* *Earlier today (January 25, 2023), it appears that the threat actor in fact posted data purportedly exfiltrated from CMMC to its "dark web" website. CMMC is investigating.* I agree with the Organization's assessment. A reasonable person would consider that 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). Further, the Organization reported "the threat actor in fact posted data purportedly exfiltrated from CMMC to its "dark web" website", increasing the risk of harm to individuals. Further, the personal information was available to the unauthorized third party for approximately five (5) weeks.

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.

The contact, identity, and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Employee file information could be used to cause hurt, harm or embarrassment. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

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). Further, the Organization reported "the threat actor in fact posted data purportedly exfiltrated from CMMC to its "dark web" website", increasing the risk of harm to individuals. Further, the personal information was available to the unauthorized third party for approximately five (5) weeks.

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 current employees and directors by email on December 29, 2022. The Organization sent a follow-up notice to current employees by email on January 5, 2023, in accordance with the Regulations. As well, the Organization notified former employees by email or mail between January 16 and January 19, 2023 and former directors by email on January 23, 2023 in accordance with the Regulations. The Organization is not required to notify the these affected individuals again

I understand that 15 affected former employees have not been notified to date as the Organization has been unable to identify contact information.

Section 19.1(1) of the Regulation states "Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must …be given directly to the individual". However, pursuant to section 19.1 (2), "…where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

Given this, and pursuant to section 37.1(2) of PIPA which states "… the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate…", **I require the Organization to report to my office within ten (10) days of the date of this decision, with what it intends to do to notify the former employees that have not been directly notified. As stated above the Organization may consider a submission under section 19.1(2) for those former employees.**

Cara-Lynn Stelmack
Assistant Commissioner, Case Management