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	Canbriam Energy Inc. (Organization)
Decision number (file number)	P2021-ND-050 (File #013140)
Date notice received by OIPC	April 26, 2019
Date Organization last provided information	April 26, 2019
Date of decision	March 2, 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 the following information: <u>Employees</u> • first and last name, • home address, • province, • postal code, • annual salary (including bonus payments and other renumeration), • birthdate (day and month, not year), • income for the year, • income tax deducted (paid), • CPP contributions, • EI premiums paid, • taxable benefits included in employee's compensation, and • last three numbers of the individual's SIN. <u>5 Former Employees and 51 Related Individuals</u> • first and last name, and • mailing address

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 26, 2019, a service provider advised the Organization that a former employee of the service provider improperly accessed and collected some of the service provider's data and uploaded it onto a remote server. • On March 15, 2019, the service provider advised the Organization that personal information of the Organization's current and former employees and related individuals was amongst the client data that was stolen from its computer network. • The service provider determined that a short term employee had surreptitiously and unlawfully downloaded data from the service provider's network from January 28, 2019 to February 20, 2019. • The individual has since been arrested and charged.
Affected individuals	The incident affected up to 3,000 individuals, including 77 current and former employees of the Organization. The service provider also indicated that an additional 56 individuals were affected by the incident; however, the Organization reviewed the list of 56 individuals and confirmed that only five (5) are former employees and the remaining 51 appear to be former consultants or surface landowners.
Steps taken to reduce risk of harm to individuals	The Organization: • Notified affected individuals. • Offered identity theft and credit monitoring services. • Reviewing agreements with service providers to ensure adequate data protection and security safeguards regarding personal information provided to service providers. The Organization reported that its vendor: • Changed passwords on systems, devices and applications. • Shut down any remote access capability. • Ongoing monitoring of inbound and outbound traffic from its systems. • Reported to law enforcement and data protection authorities. • Notified affected individuals. • Investigated to determine the scope of the individual's wrongdoing; and

	• Engaged third-party forensic consultants to assist with the investigation.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on March 27, 2019 and again on April 10, 2019.
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, "there is a risk of identity theft, fraud and financial loss to the employees in question, in addition to humiliation and embarrassment of having employment compensation information potentially disclosed." Further, "For the five Former Employees and fifty-one Related Individuals whose name and mailing address were potentially disclosed and accessed as part of the Incident, [the Organization] is of the view that those individuals are not at risk of any type of harm arising out of the Incident." I agree with the Organization's assessment. A reasonable person would consider that the identity, tax and employment information at issue could be used to cause the significant harms of identity theft, fraud and financial loss, as well as hurt, humiliation and embarrassment. Name and mailing address alone cannot generally be used to cause significant harm.
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.	In summary, the Organization reported: • The former employee has been arrested and the stolen data has been recovered. • There is no evidence indicating the information at issue was further disseminated or disclosed prior to being recovered, although "similarly there is no confirmation that it has not been disseminated or disclosed". • The fact the incident resulted from theft increases the likelihood of harm to affected individuals. • The Organization and its service provider have taken steps to minimize the likelihood of harm. In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of almost a month; it is not clear how long after this that the former employee was arrested. Although the Organization reported there is no evidence the information was further disseminated or disclosed prior to being recovered, this cannot be known for sure.

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, tax and employment information at issue could be used to cause the significant harms of identity theft, fraud and financial loss, as well as hurt, humiliation and embarrassment. Name and mailing address alone cannot generally be used to cause significant harm. The likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of almost a month; it is not clear how long after this that the former employee was arrested. Although the Organization reported there is no evidence the information was further disseminated or disclosed prior to being recovered, this cannot be known for sure. 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 that affected individuals were notified in writing on March 27, 2019 and again on April 10, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner