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	EBM Geoscience Inc. (Organization)
Decision number (file number)	P2021-ND-337 (File #021666)
Date notice received by OIPC	June 11, 2021
Date Organization last provided information	June 11, 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 is located 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: • business contact information, • driver's license, • social insurance number, and • financial information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the personal information appears to be business contact information, which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e-mail address, business fax number and other similar business information". Section 4(3)(d) of PIPA says that the Act does not apply to "the collection, use or disclosure of an individual's business contact information if the collection, use or disclosure, as the case may be, is for the purposes of enabling the individual to be contacted in

	relation to the individual's business responsibilities and for no other purpose". In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business and for no other purpose." As such, the information is not excluded from the Act and PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization was the victim of a business email compromise. • The incident was discovered on or about May 19, 2021, when the Organization's bank representatives inquired about email address changes and a wire transfer authorization request. • An investigation determined that two organizational email accounts were compromised as early as May 15, 2021, and were used to initiate fraudulent wire transfers. • The Organization did not report how the email accounts were compromised.
Affected individuals	The incident affected 6 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Secured the affected email accounts. • Retained external IT and cybersecurity experts to investigate the incident and provide security recommendations. • Reinforced passwords and setup multifactor authentication. • Offered affected individuals credit monitoring and identity theft protection services.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally or by email on May 19 and June 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: *Considering the type of information at issue, the potential harms may include identity theft, fraud and email phishing.* I agree with the Organization's assessment. A reasonable person would consider that the contact, 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 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 that "There is a possibility that the harm described … could materialize, given the nature of the incident." 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 a third party (deliberate intrusion, supply chain attack by way of email fraud). Further, the email accounts were compromised for approximately 4 days.

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 contact, 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 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, supply chain attack by way of email fraud). Further, the email accounts were compromised for approximately 4 days.

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 verbally or by email on May 19 and June 11, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner