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	Insurance Bureau of Canada (Organization)
Decision number (file number)	P2021-ND-263 (File #020921)
Date notice received by OIPC	February 12, 2021
Date Organization last provided information	November 5, 2021
Date of decision	February 9, 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 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: <u>Vendors:</u> • electronic fund transfer information, and • business contact information. <u>Current and former employees:</u> • name, • social insurance number, and • date of birth. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that 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(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "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 unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities 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	• On January 28, 2021, an unknown third party temporarily gained unauthorized access to the email account of an employee of the Organization through a targeted email phishing campaign. • On February 3, 2021, the unauthorized individual subsequently used the account to send phishing messages to certain contacts in the employee's mailbox. • On February 4, 2021, the Organization alerted recipients of the February 3, 2021 message that it could pose a security risk and should not be opened. • The Organization reported it has no evidence at this time that any information was viewed or used in any way as a result of this incident.
Affected individuals	The Organization reported the incident affected approximately 1,500 vendors, as well as 26 current and former employees in Alberta.
Steps taken to reduce risk of harm to individuals	• Took immediate action to secure the affected account and commenced an investigation with the assistance of outside cybersecurity experts. • Providing current and former employees with free credit monitoring protection for two years, as well as information about steps they can take to protect their information. • Reviewing and enhancing controls to help reduce the risk of such incidents in future. • Plan to conduct mandatory enhanced cyber resiliency training for all staff.

Steps taken to notify individuals of the incident	Affected individuals were notified by letter on February 18, 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 it "…has identified a potential risk of harm of phishing and identity theft or fraud in relation to this incident." The Organization also reported: *For the employees and former employees who were potentially affected, [the Organization] is providing individuals with free credit monitoring protection for two years, as well as information about what steps they can take to protect their information.* In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used for the purposes 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 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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident, although it reported it "…has no evidence at this time that any of this information has been viewed or used in any way as a result of this incident." In my view, 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). The personal information at issue was used to send phishing emails.
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 for the purposes 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 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). The personal information at issue was used to send phishing emails.	

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by letter on February 18, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner