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	Koelnmesse (Organization)
Decision number (file number)	P2021-ND-315 (File #021679)
Date notice received by OIPC	June 14, 2021
Date Organization last provided information	June 14, 2021
Date of decision	March 7, 2022
Summary of decision	There is a real risk of significant harm resulting from 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 based in the state of Illinois and organizes trade shows throughout the United States. 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: • credit/debit card number, • expiration date, • CVV/security code, and • electronic/digital signature. This information is about an identifiable individual 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 February 23, 2021, the Organization became aware of a possible data security incident involving its computer network. • The Organization determined that an unauthorized individual accessed an employee's email account from January 26, 2021 to February 23, 2021.

	• The Organization retained a third-party vendor to review the impacted information. The review was completed on May 7, 2021 and determined that the personal information of one (1) Alberta resident might be impacted. • The Organization reported that is not aware of any misuse of personal information because of the incident, but out of an abundance of caution, is providing notification of this incident to individuals whose information may have been impacted.
Affected individuals	The incident affected one (1) individual whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Took immediate steps to secure its systems and investigated. • Implemented measures to enhance the security of its environment in an effort to minimize the likelihood of a similar event from occurring in the future. • Improved its email gateway requiring certain files to be quarantined prior to being allowed in the network. • Introduced quarterly technology meetings to train employees about phishing and other email issues. • Reported the incident to the United States Federal Bureau of Investigation.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on June 16, 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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated: *You should follow the recommendations given further below to ensure that your personal information is protected, including reviewing your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the card immediately.* In my view, a reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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 did not specifically provide its assessment of the likelihood of significant harm resulting from this incident, but it did report that it "… is not aware of any misuse of personal information 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. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, it appears the email account was exposed for approximately one month.

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 individual.

A reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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 an unknown third party. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, it appears the email account was exposed for approximately one month.

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 individual by letter on June 16, 2021 in accordance with the Regulations. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner