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	Kohl Children's Museum of Greater Chicago (Organization)
Decision number (file number)	P2020-ND-192 (File #016904)
Date notice received by OIPC	August 17, 2020
Date Organization last provided information	November 18, 2020
Date of decision	December 16, 2020
Summary of decision	There is a real risk of significant harm to the individuals affected by 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 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: • name, • address, • social security number, and • financial account information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On July 16, 2020, the Organization received notice that its third-party cloud computing provider, Blackbaud, had been the target of a ransomware attack in May 2020.

	• The Organization reported that Blackbaud reported that data was exfiltrated by the unknown actor at some point before Blackbaud locked the unknown actor out of the environment on May 20, 2020. • On or about August 5, 2020, the Organization received further information from Blackbaud that allowed it to confirm the information potentially affected may have contained personal information.
Affected individuals	The incident affected a total of 464 individuals, including 1 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	The Organization: • Worked with Blackbaud to understand the scope of the incident and identify the affected information. • Notified affected individuals and provided information on how to protect their personal information, including providing complimentary credit monitoring services for twelve months. • Is reviewing existing policies and procedures regarding third-party vendors. • Is working with Blackbaud to evaluate additional measures and safeguards to protect against similar incidents in the future. The Organization reported its service provider: • Reported the incident to law enforcement and worked with forensic investigators to investigate • Notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on August 17, 2020.
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 possible harms that might result from the incident are "Potential identity theft or fraud". 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 significant harms of identity theft and fraud.

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: *Based on the type of data potentially impacted, the capability of the data to be used to commit identity theft or fraud, the extent of the personal information involved, the type of cyber incident, and the exfiltration of the data from the Blackbaud systems by the unauthorized actor, there is a moderate likelihood of potential harm to impacted individuals.* I agree with the Organization's assessment. A reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized action, ransom demand) and the information was exfiltrated.

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 significant harms of identity theft and fraud. The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized action, ransom demand) and the information was exfiltrated.

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 affected individuals by letter on August 17, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner