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	Ivanhoe Cambridge (Organization)
Decision number (file number)	P2021-ND-099 (File #013428)
Date notice received by OIPC	June 19, 2019
Date Organization last provided information	June 19, 2019
Date of decision	March 31, 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 the 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • email address, • delivery information (name, telephone number, and address), • billing information (name, telephone number, and address), and • credit card information. This information is about identifiable individuals 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 June 13, 2019, the Organization's third party service provider, responsible for maintaining its ecommerce platform, noticed an unauthorized script.

	• The Organization investigated and determined an unauthorized third party gained access to the ecommerce platform and placed a script allowing personal information to be collected as transactions were made on the site. • The unauthorized third party was able to access the ecommerce platform remotely by using the username and password of an employee of the Organization. • The incident affected purchases made between June 10, 2019, and June 13, 2019.
Affected individuals	The incident affected 8 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• The third party service provider removed the malware and informed the Organization. The parties investigated to determine the root cause of the issue. • Informed payment processors. • Changed the employee's compromised credentials and audited devices. Changed other ecommerce employees' credentials. • Implemented new security measures.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on June 14, 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 "Affected individuals were informed that their personal information had potentially been accessed by an unauthorized third party and that this could increase the risk for fraud and phishing attempts". In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes, increasing 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 the likelihood of harm resulting from this incident is "Unknown". In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the incident appears to be the result of malicious intent (compromised credentials). The information was exposed for three 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 and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting in this case is increased because the incident appears to be the result of malicious intent (compromised credentials). The information was exposed for three 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 affected individuals were notified by email on June 14, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner