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	Marval Capital Ltd. (Organization)
Decision number (file number)	P2020-ND-069 (File # 015700)
Date notice received by OIPC	April 23, 2020
Date Organization last provided information	April 23, 2020
Date of decision	July 15, 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 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported it is "… not able to determine which emails were accessed besides the ones used for phishing. Some phishing emails contained some or all of the following items; email address, name, address, account information and phone number". 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 March 24, 2020, the Organization's general email account was used to send out phishing emails.

	• The person that accessed the account had brief access to the inbox. The Organization and its email provider were not able to determine which emails the intruder may have opened in that time. • The Organization reported the breach "occurred during the COVID-19 pandemic during the Organization's transition to working remotely as mandated by the Federal Government". • The breach was discovered the same day when the Organization noticed unusual activity with its general email account.
Affected individuals	The incident affected 13 individuals.
Steps taken to reduce risk of harm to individuals	• Immediately took steps to block the unauthorized access and secure information. • Reset passwords on accounts. • Closed the compromised email account. • Consulted a cyber security firm. • Conducting daily monitoring and alerts of suspicious activity, fraudulent transactions, address updates to accounts and many other features. • Enhancing security for email, protection against viruses on devices and further securing cloud data. • Communicated with "the whole company about the event". • Offered affected individuals complimentary 12-month subscription for credit monitoring.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 24, 2020 and April 1, 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 did not specifically identify potential harm(s) that might result from the incident, but reported "The likelihood of any personal information being extracted from the body of emails and used is low". In my view, a reasonable person would consider the contact and financial information potentially at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to 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	The Organization reported "From speaking with security specialists and lawyers the likelihood of any personal information being extracted from the body of emails and used is low".

cause and effect relationship between the incident and the possible harm.	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 compromised email account 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 the contact and financial information potentially at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. 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 compromised email account was used to send phishing emails.

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 affected individuals were notified by email on March 24, 2020 and April 1, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner