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	Avenue Living Asset Management Ltd. (Organization)
Decision number (file number)	P2021-ND-306 (File #019106)
Date notice received by OIPC	January 20, 2021
Date Organization last provided information	January 20, 2021
Date of decision	March 3, 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 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 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 Organization reported the incident involved the following information: • first and last name, and, • corporate email address. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. "Business contact information" 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 possible 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 a result, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 26, 2020, an employee with the Organization unknowingly clicked on a phishing link sent to her by email, which in turn allowed an unauthorized actor to gain access to the employee's email account and subsequently send a phishing link to the employee's contacts via email. • The breach was discovered the same day after multiple emails were sent from the employee's account, and various replies were received. • The Organization reviewed all emails and determined that all of the emails were corporate email accounts.
Affected individuals	The incident affected 478 individuals, including approximately 8 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Sent a notification to each unique email address affected. • Locked the employee's email account. • Changed login information for the employee's accounts to prevent any further potential unauthorized access. • Investigated and confirmed that the only unauthorized email phishing scam was in connection with the employee's email account. • Implemented a Multi-Factor-Authentication requirement to increase account security. • Taking steps to help prevent an incident of this nature from occurring in the future, including the implementation of a comprehensive and mandatory company-wide training regarding phishing and cyber attacks.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on November 27, 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	The Organization reported, *This incident presents a real risk of significant harm to the affected individuals. For all unique emails [sic] addresses inadvertently disclosed, the affected individuals corporate email accounts will be at increased risk of unsolicited emails, phishing*

non-trivial consequences or effects.	*scams or SPAM email. Individuals whose full names were exposed are at a potential risk of identity theft.* I agree with the Organization's assessment. A reasonable person would consider that the email addresses could be used for the purposes of phishing, 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, *There is a real risk of significant harm in this case. The incident resulted from malicious intent. It is possible that the information described above has been further distributed.* I agree with the Organization's assessment. 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, phishing). Additionally, the Organization reported the information was used to send additional 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 email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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 (deliberate intrusion, phishing). Additionally, the Organization reported the information was used to send additional 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 the Organization notified the affected individuals by email on November 27, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner