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 Communities Ltd. (Organization)
Decision number (file number)	P2020-ND-059 (File #014961)
Date notice received by OIPC	February 7, 2020
Date Organization last provided information	February 7, 2020
Date of decision	May 29, 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 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: • name, • residential address, • email address, • telephone number, • date of birth, • social insurance number, • medical information, • residential lease, • pre-authorized debit agreement, • direct deposit form, • scanned copy of two personal cheques, • bank account number, • monthly rent amount, and • insurance information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On December 17, 2019, the Organization became aware that an unknown and unauthorized actor had altered an employee's email account settings to automatically forward all incoming emails to an unrecognized email address. • The Organization determined that all emails received by the employee on or after October 23, 2019 until December 17, 2019 had been automatically forwarded to the unrecognized email address. • The total number of emails forwarded totalled 3,667. The Organization reviewed each of the 3,667 emails and determined that personal information of 262 individuals (including four employees) were contained within the emails. • The Organization discovered the breach on December 17, 2019 as the result of an automated warning from the email server provider. • Organization was not able to conclusively determine the method by which the unauthorized actor gained access to the employee's email account, but suspects that their password may have been compromised.
Affected individuals	The incident affected 262 individuals of which 248 were residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Locked the employee's email account and began an investigation. Confirmed that the only unauthorized email forwarding issue was in connection with the sole employee's email account. • Removed the forwarding rule. • Changed login information for the employee's accounts to prevent any further potential unauthorized access. • Will provide retraining for the employee and other employees regarding the importance of password safety and the protection of personal information. • Reconfiguring reports that include residential addresses to only include anonymized building codes.
Steps taken to notify individuals of the incident	The affected individuals were notified by letter on February 5, 2020 and by email on February 6, 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: *This incident presents a real risk of significant harm to the affected individuals. Where medical information was disclosed, the harm to the affected individuals could result in humiliation. For all unique emails addresses inadvertently disclosed, the affected individuals will be at increased risk of unsolicited emails, phishing scams or SPAM email. Individuals whose additional personal details were disclosed (ie, SIN, legal name, physical address, etc) are at heighted risk of identity theft. Finally, for those individuals whose banking information was disclosed, there is a risk that such information could be used to make unauthorized withdrawals from their accounts or in sophisticated phishing attempts that reference their correct account number.* I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, financial and insurance information at issue could be used to cause the harms of identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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 has been further distributed." 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 (deliberate intrusion into an employee's email account). Further, the information may have been exposed for approximately two months.
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, financial and insurance information at issue could be used to cause the harms of identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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 into an employee's email account). Further, the information may have been exposed for approximately two months.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by letter on February 5, 2020 and by email on February 6, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner