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 (2014) LP (Organization)
Decision number (file number)	P2017-ND-167 (File #007373)
Date notice received by OIPC	December 13, 2017
Date Organization last provided information	December 14, 2017
Date of decision	December 22, 2017
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a limited partnership which operates in Alberta and is an "organization" as defined in section 1(1)(i)(iv) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported that it "does not know the personal information compromised by this incident. Only CPS has that information." However, the Organization "assumes that the breach relates to personal information of its clients/tenants obtained by the organization through its application and lease process." The Organization submitted a "blank copy of [its] standard application form" to the Office of the Information and Privacy Commissioner (OIPC) with its report of the breach, and noted that: *In general, the information included in such applications is:* • *Name,* • *Address,* • *Date of birth,* • *Email address,* • *Social insurance no.* I find that this information is about identifiable individuals and qualifies as "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.

DESCRIPTION OF INCIDENT	
☒ loss ☐ unauthorized access ☐ unauthorized disclosure	
Description of incident	• The Organization reported that on or about November 2, 2016, Calgary Police Services (CPS) informed the Organization that it was conducting a criminal investigation concerning the fraudulent use of personal information to apply for credit cards and there was a possible connection to approximately 40 individuals through a relationship with the Organization. • The Organization confirmed to the CPS that approximately 30 of the persons identified by the CPS were tenants of the Organization. • On November 29, 2016 the Organization received an update from the CPS regarding CPS's ongoing investigation. That same day, the Organization initiated "an internal privacy control investigation" and "identified that an unknown person had accessed the [Organization's] server after hours]." • The Organization informed CPS, and CPS confirmed to the Organization that "an Employee was accessing the server on a personal device and had stolen certain tenant personal information from [the Organization]". The Organization "understands from CPS that the Employee had the stolen personal information from [the Organization] and kept it on a computer at his home address and sold the stolen personal information for personal gain." • The Organization reported that during its discussion with the CPS on November 29, 2016, "CPS would not disclose the nature of the personal information which had been taken, given that the matter was under a current criminal investigation." • The Organization reported that it "does not know precise details of when the loss occurred. To the best knowledge of the organization, the loss occurred sometime between August, 2016 and November, 2016."
Affected individuals	The Organization reported that when it was initially contacted by CPS, it initially "confirmed that 30 persons on that list had a tenant connection" to the Organization. After being informed on December 6, 2017 that a complaint had been submitted to the OIPC, the Organization requested the OIPC provide the names of affected individuals. The OIPC does not have this information and advised the Organization to contact CPS to obtain the names of affected individuals.

	The Organization contacted CPS and, on December 13, 2017, was "provided the names of the affected individuals associated with [the Organization]. The lists identify 30 individuals who have been impacted in this matter, inclusive of [the individual who complained to the OIPC]."
Steps taken to reduce risk of harm to individuals	The Organization reported that it has taken the following harm reduction steps since it became aware of the breach: • *Immediate termination of the Employee upon discovering the breach;* • *Retained a third party service provider… to conduct a full review of the organization's collection and retention policies and practices relating to confidential and personal information;* • *Retained outside counsel to assist it in responding to this matter and ensuring full compliance with Alberta privacy and personal information legislation; and* • *Initiated privacy controls with IT Department inclusive of automatic password changes; limit on call center personnel accessing data on the server; daily/weekly review of server after hour access by IP address.*
Steps taken by the organization to notify individuals of the incident	The Organization reported that: *When [the Organization] was contacted by CPS, it was told that CPS had/would contact the affected individuals about this matter so they could take appropriate precautions. At that time, [the Organization] understood that all efforts had been made by CPS to contact affected individuals and notify each of them that their personal information was being used fraudulently and that should they have any questions to contact [the Organization]. [The Organization] did not have an understanding that it was statutorily required to issue a notice of this kind to the Office of the Information and Privacy Commissioner of Alberta, or to send an additional notice to the affected individuals.* *Since [the Organization] has become aware of these issues, it has:* • *Undertaken an internal review of all information and communication related to this matter in an attempt to determine the identity of the affected parties;* • *Requested disclosure of the names of the affected parties from the Office of the Information and Privacy Commissioner of Alberta; and*

	• *Requested disclosure of the names of the affected parties from CPS.* The Organization is aware, as a result of a complaint filed with the OIPC, that an individual "has been impacted by this matter and had certain fraudulent credit accounts opened in her name." The Organization contacted this individual on August 10, 2017. Further, the Organization reported that it "has just uncovered a list of the affected individuals and is presently trying to determine their current contact information."
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.	In its report of the breach, the Organization said that it… *…believes there is a significant risk of harm to individuals as a result of this breach. The most significant risks of harm include:* • *Financial fraud* • *Identity theft* • *Hurt, humiliation or damages to reputation or relationships* In my view, the personal information reportedly collected by the Organization through its application and lease process includes identity information that could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for phishing purposes, which in previous breach notification decisions I have found to be a significant harm.
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.	As noted, the Organization said that it "…believes there is a significant risk of harm to individuals as a result of this breach." The Organization also reported that it … *…does not know:* • *Exactly what personal information has been compromised;* • *How widely the personal information was disseminated;* • *How long the personal information has been exposed; or* • *Whether all impacted individuals have been notified by CPS such that they may take, or have taken protective steps.*

	Given the risk of significant harm in this instance, [the Organization] believes that all affected individuals should be notified of this incident as soon as possible and the organization requests the assistance of the commissioner's office in that regard. In my view, there is a real risk of significant harm in this case. The incident resulted from malicious intent – that is, a (now former) employee has reportedly stolen the personal information, "sold the stolen personal information for personal gain", and has now been criminally charged. The Organization is aware of at least one individual who "had certain fraudulent credit accounts opened in her name." It is possible that the information has been exposed since April 2016, and has reportedly been further distributed.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information before me and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

The personal information reportedly collected by the Organization through its application and lease process includes identity information that could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for phishing purposes, which in previous breach notification decisions I have found to be a significant harm.

The incident resulted from malicious intent: a (now former) employee reportedly stole the personal information, "sold the stolen personal information for personal gain", and has now been criminally charged. The Organization is aware of at least one individual who "had certain fraudulent credit accounts opened in her name." It is possible that the information has been exposed since April 2016, and has reportedly been further distributed (sold).

The Organization reported that it "did not have an understanding that it was statutorily required to issue a notice of this kind to the Office of the Information and Privacy Commissioner of Alberta, or to send an additional notice to the affected individuals" and that it understood that the CPS "had/would contact the affected individuals about this matter so they could take appropriate precautions".

I want to emphasize that the requirement under section 34.1 of PIPA is that "**An organization having personal information under its control** must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure."

Pursuant to section 37.1(1) of PIPA, where an organization is required to provide notice under section 34.1, I "may require **the organization** to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure...".

In this case, I require the Organization to notify the approximately 30 individuals known to be affected by this incident in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and **notify me in writing that it has done so on or before January 5, 2018.**

Further, section 37.1(2) of PIPA states that "If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1)."

Pursuant to section 37.1(2), I require the Organization to consider whether or not there may be additional affected individuals, beyond those who may have been identified by the CPS to date. That is, the Organization is aware, as a result of receiving information from CPS, that personal information of some individuals was accessed by a (now former) employee, stored on a home computer, and sold. Information appears to have been recovered by police. However, I am concerned that the employee may have had access to the personal information of other individuals while still an employee of the Organization, and those individuals may also be at risk, even though their personal information was not recovered by police. I require the Organization to consider this scenario and advise me as to its assessment of the potential risk to other individuals, beyond those already identified by police.

The Organization is required to provide me with its assessment of this possible additional risk, **in writing, on or before January 5, 2018.**

Jill Clayton
Information and Privacy Commissioner