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)	P2018-ND-049 (File #007373)
Date notice received by OIPC	December 13, 2017 (date original notice of breach received by the OIPC)
Date Organization last provided information	February 7, 2018
Date of decision	April 18, 2018
Summary of decision	On December 22, 2017, I issued breach notification decision P2017-ND-167, requiring the Organization to notify approximately 30 individuals known to be affected by this incident, and to notify me in writing on or before January 5, 2018 that it had done so. On January 5, 2018 I received confirmation that the individuals had been notified. Breach notification decision P2017-ND-167 also required the Organization to consider whether or not there may be additional affected individuals, beyond the 30 already identified. The Organization was required to provide me with its assessment of this possible additional risk, in writing, on or before January 5, 2018. I received the Organization's submissions assessing possible additional risk on January 5, 19 and February 7, 2018. Having reviewed these submissions, I find that a reasonable person would consider that there is a real risk of significant harm to additional individuals as a result of 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 its former employee had access to rental application forms, tenant management software and tenant lease agreements. The available information includes:

	• *Name,* • *Address,* • *Phone number,* • *Date of birth,* • *Email address,* • *Social insurance number,* • *Signatures* 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	Breach notification decision P2017-ND-167 describes the incident. In summary: • 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 a number of individuals who had a relationship with the Organization. • The Organization's internal investigation, and information provided by CPS, confirmed that an employee of the Organization (now former employee) accessed the Organization's server after hours using a personal device, stole certain tenant personal information, and subsequently sold the information for personal gain. • The Organization believes the unauthorized access occurred sometime between August 2016 and November 2016. The Organization's January 5, 19 and February 7, 2018 submissions assessing possible additional risk provided the following additional information: • The former employee was employed with the Organization from August 2015 to December 5, 2016. • The former employee performed minor data entry functions and had access to work orders for repairs or complaints about other tenants or property. The former employee also had access to residential lease agreements (hard copy).

	• The former employee did not have authorized access to the Organization's server. Nonetheless, the former employee accessed the server after hours using a personal device. The server contained lease application forms which include name, address, date of birth, email addresses, social insurance numbers and signatures. The lease applications were not encrypted. • The Organization was unable to confirm how many lease application forms were on the server during the former employee's period of unauthorized access. • The Organization has limited information from the CPS regarding how the personal information was accessed and what was taken as the matter is currently before the criminal courts.
Affected individuals	The Organization reported that 30 individuals are known to be affected by this incident. The Organization did not estimate the number of additional individuals who might be affected.
Steps taken to reduce risk of harm to individuals	The Organization reported that it has taken the following "protectionary measures" since the incident was discovered: • Terminated 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 to notify individuals of the incident	The Organization notified approximately 30 individuals known to be affected by this incident by letter sent January 4, 2018.
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 January 5, 19 and February 7, 2018 submissions, the Organization reported that "Common data entry tasks for a call center agent would include accessing tenant management software and inputting work orders, such as tenant requests for repairs or complaints about other tenants of the property." The data resides in a server hosted in Chicago "and all personal and private information such as bank account and social insurance numbers are encrypted in the database-this information is not visible to anyone".

	With respect to lease agreements, the Organization reported that "Other than the tenant's name, there is no personal information contained in these hard copy documents". The Organization also said "The detailed account information of the Organization's tenants is encrypted and cannot be viewed or verified, even with authorized access to the server. The tenant lease application forms on the server were not encrypted…". Given these submissions, I agree with the Organization that it is unlikely that personal information the former employee may have accessed in the course of his data entry responsibilities, and the limited personal information found in standard form lease agreements, could be used to cause significant harm. Residential lease application forms stored on the Organization's server, however, contain personal information that could be used to cause significant harm. In breach notification decision P2017-ND-167, I said that identity information (such as date of birth, social insurance number, etc.) could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for phishing purposes, which I have previously said a reasonable person would consider 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.	In assessing the likelihood of harm to individuals, other than the 30 already identified, the Organization said: • *Sometime between August 2016 and November 2016, a call centre employee of the Organization accessed the Organization's server after hours with malicious intent and took the personal information of 30 individuals associated with the Organization.* • *The detailed account information of the Organization's tenants is encrypted and cannot be viewed or verified. The tenant lease application forms on the server were not encrypted, though access to the server was password protected and only accessible through a secure network;* • *Upon discovery of this incident, the Organization implemented a number of additional protections and safeguards…. None of these safeguards have been "triggered';*

	• *CPS conducted a thorough investigation with full participation by the Organization. The results of that investigation were that 30 individuals of the Organization had their personal information breached by the rogue employee. CPS further confirmed it did not have any evidence or information to suggest that further individuals of the Organization were impacted;* • *The investigation of the Organization, which was conducted with the assistance of both CPS and IT specialists, did not reveal any information or evidence to suggest that any personal information other than that of the 30 individuals known to be affected had been compromised, and* • *The Organization has not been contacted by any individuals other than a select few of those known to be affected with respect to any concerns of this matter or of a potential privacy breach. The Organization maintains monthly contact with all tenants and maintains a 7 day a week call center.* The Organization submits that "there is no evidentiary basis, beyond speculation or conjecture, to assert that further individuals of the Organization were affected by this matter. As such, there is no significant risk of harm to any further individuals of the Organization and no further notification is required." Despite the Organization's submissions, in my view a reasonable person would consider there is a real risk of significant harm to those individuals whose personal information was in lease application forms on the server at the time the former employee had unauthorized access, for the following reasons: • The server was accessed by an unauthorized employee with malicious intent and for criminal purposes. • The incident "occurred sometime between August, 2016 and November, 2016", an exposure period of three months. • The Organization has repeatedly said that its investigation "did not reveal any information or evidence to suggest that any personal information other than that of the 30 individuals known to be affected had been compromised".

	However, despite making three submissions assessing the possibility of additional risk, the Organization has not, or cannot, definitively state that the unauthorized former employee only accessed the information of 30 individuals. It appears the Organization did not have the audit capability to confirm what information was accessed by the unauthorized IP address reportedly associated with the former employee. The Organization has not confirmed that the former employee did not access anyone else's information. • The protectionary measures undertaken by the Organization after the incident do not assist me in assessing the risk that the former employee may have accessed the information of additional individuals during the unauthorized access to the server. The fact that the Organization has not been contacted by any other affected individuals does not mean additional information was not accessed or will not be used for unauthorized purposes in the future. My decision in this matter is consistent with a number of breach notification decisions previously issued by my Office which have found a real risk of significant harm in circumstances where an organization had no information or evidence that information was accessed without authorization, but could not rule such access out (see by way of example only, P2011-ND-001; P2011-ND-003 at paras. 16-17; P2013-ND-23; P2016-ND-51; P2017-ND-77; P2017-ND-78; P2017-ND-83).

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information before me and given the circumstances of the incident, in my view a reasonable person would consider there is a real risk of significant harm to those individuals whose personal information was stored in lease application forms on the server at the time the former employee had unauthorized access.

The likelihood of harm resulting from this incident is increased because personal information on the server was accessed by an unauthorized employee with malicious intent and for criminal purposes. The exposure may have occurred over three months. The Organization cannot confirm what information was accessed from the unauthorized IP address reportedly associated with the former employee. Protections the Organizations put in place after the incident do not address the risk that the former employee may have accessed the information of additional individuals during the unauthorized access to the server. The fact that the Organization has not been contacted by any other affected individuals does not mean additional personal information was not accessed or will not be used for unauthorized purposes in the future.

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

The Organization reported that direct notification would not be possible because it does not have current contact information for all individuals potentially impacted by this matter. It states that it has a very high turnover rate for tenants and the incident occurred sometime on or before November 2016. The Organization reports that it operates in Brooks, Camrose, Edmonton, Lethbridge, Lloydminster, Medicine Hat and Wetaskiwin. It proposes to issue indirect notification to potentially affected Alberta residents by publishing a notice in a local newspaper of each municipality where it operates. The Organization does not believe that a notice posted on its website would be an effective form of indirect notice because its website is directed towards new potential clients or partners (who would not have been impacted by this matter).

I accept that indirect or substitute notice as proposed by the Organization is reasonable where the Organization does not have current contact information for affected individuals. In addition, since individuals may have moved out of those municipalities, I require the Organization to post a general notification about the breach on its website for a period of 30 calendar days. However, where the Organization has current contact information, the Organization is required to notify individuals directly.

The Organization is required to confirm to me in writing on or before May 4, 2018 that it has notified affected individuals as described above.

Jill Clayton
Information and Privacy Commissioner