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	Boardwalk Rental Communities (Organization)
Decision number (file number)	P2020-ND-167 (File #015915)
Date notice received by OIPC	May 26, 2020
Date Organization last provided information	October 30, 2020
Date of decision	December 1, 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 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 information of four (4) individuals contained in "Offer of Lease" documents: • first and last name, • date of birth, • current address, • landlord's name, • telephone number, • email address, • employer and occupation, • annual income, • emergency contact and phone number, • one (1) individual's social insurance number. The incident also involved the following information of two (2) individuals included in "Move Out Packages"" • first and last name, and • forwarding address.

	The information of five (5) individuals was included in three (3) Renewal Packages, as follows: • first and last name, • address, • lease term, and • monthly rent and incentives. The incident also involved a logbook containing employee names and shifts worked, a notebook of unknown content but which may include information relating to select suites and telephone numbers, and a cellphone and Sonim device (similar to a cellphone), which contains personal information but is secured by passcodes. 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 May 18, 2020, an unknown individual entered the leasing office at the Organization's Viking Arms location. • A number of items were stolen including documents, a cellphone, a debit card machine, log book, a note book and a Sonim.
Affected individuals	The incident affected 7 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted an investigation. • Contacted law enforcement. • Provided credit monitoring for one year to individuals whose Offers of Lease were stolen. • Password protected the cellphones in question. • Cancelled the cellphone's SIM card. • Marked the IMEI as stolen. • Issued a device wipe demand. • Asked staff to change their passwords. • Looking into software solutions to ensure all documents are signed electronically to reduce the number of documents stored on site. • Reviewing security protocols to increase security patrols. • Looking at solutions for installation of improved security alarms.

Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and letter on May 22, 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 "The identity information could be used to cause the significant harm of identity theft and fraud." I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and employment information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, 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 cause and effect relationship between the incident and the possible harm.	The Organization reported, *The likelihood of harm resulting from this incident is increased as it was a result of malicious intent (theft). None of the documents have been recovered. The risked is mitigated by the Sonim and cellphone being password protected and risk mitigation steps taken...* On October 30, 2020, the Organization provided an update, reporting that the "missing documents" were returned by an unknown individual between July 31, 2020 and August 1, 2020. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). Although the documents have been returned, it is not clear whether the documents were viewed, copied, or redistributed, and they were exposed for over two months. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, although the cellphones and Sonim device were password protected, they were not encrypted.
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 and employment information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). Although the documents have been returned, it is not clear whether the documents were viewed, copied, or redistributed, and they were exposed for over two months.	

Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, although the cellphones and Sonim device were password protected, they were not encrypted.

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

I understand the Organization notified affected individuals by telephone and letter on May 22, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner