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	Tyrell Inc. o/a Zentrum (Organization)
Decision number (file number)	P2018-ND-141 (File #010182)
Date notice received by OIPC	October 25, 2018
Date Organization last provided information	October 25, 2018
Date of decision	November 14, 2018
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 whose 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 Ontario based property management firm and an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • date of birth, • address, • telephone number, • email address, • employment history, • rental history, • references, • income, and • social insurance number (in some cases). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On September 26, 2018, the Organization discovered that a website it owned and operated (www.quinetrentals.com) had been accessed by an unknown party. The website is an application platform; people use the website to apply for rental accommodations. • The unknown party downloaded the personal information of people who has used the website between December 5, 2005 and September 19, 2018 and threatened to publish the information unless a ransom was paid. The Organization paid the ransom. • The incident was discovered on September 26, 2018.
Affected individuals	The incident affected 10,062 individuals; 72 individuals were or are potentially residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Deactivated the website and wiped the server hosting it. • The third party services provider hosting the website investigated the breach and confirmed that its systems and network were secure. • Will install additional security features once the website is reactivated, including a feature to automatically ensure that any personal information entered is automatically deleted from the website and server once the application has been processed. • Will offer complimentary credit and identity theft monitoring for one year to all affected individuals.
Steps taken to notify individuals of the incident	• All affected individuals were notified by e-mail or mail commencing October 24, 2018. • Posted a notice on the website.
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 that "there is a risk of phishing, identity theft and fraud". In my view, a reasonable person would consider the identity, contact, employment and rental information could be used to cause the harms of identity theft and fraud. In addition, email address and profile information could be used for phishing purposes. 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	The Organization reported: *There is a potential that the harm of phishing an identify [sic] theft could result, but there are factors which suggest any potential harm may not arise.*

between the incident and the possible harm.	*Although the information was obtained maliciously, the Hacker has undertaken not to release the information if the ransom was paid. [The Organization] retained a security expert to handle the negotiation The security expert has opined that there is a real possibility that Hacker will honour this commitment. The Hacker has a history of hacking property management companies and provided "references" to support his promise that the Information would be deleted and not published if not paid…* In my view, 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 and ransom demand). The Organization does not know how long the information was exposed. Despite receiving assurances from the unauthorized party and a security expert that the personal information would be deleted and not published (further disclosed), the fact remains that these assurances were given by individual(s) who deliberately accessed the information without authority, made ransom demands, and accepted payment of a ransom. These factors weigh heavily against accepting or trusting their assurances.

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 the identity, contact, employment and rental information could be used to cause the harms of identity theft and fraud. In addition, email address and profile information could be used for phishing purposes. 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 and ransom demand). The Organization does not know how long the information was exposed. Despite receiving assurances from the unauthorized party and a security expert that the personal information would be deleted and not published (further disclosed), the fact remains that these assurances were given by individual(s) who deliberately accessed the information without authority, made ransom demands, and accepted payment of a ransom. These factors weigh heavily against accepting or trusting their assurances.

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 all affected individuals were notified by e-mail or mail commencing October 24, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner