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	Emerald Management & Realty Ltd. (Organization)
Decision number (file number)	P2017-ND-99 (File #001856)
Date notice received by OIPC	November 9, 2015
Date Organization last provided information	February 25, 2016
Date of decision	July 18, 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 incorporated in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved photographs of completed rental application forms and credit bureau reports, which include all or some of the following information: • name, • address, • email address, • telephone number, • occupation, • date of birth, • social insurance number, • credit card number, • residential history, • banking information, • dirver's license number, • employment history, • credit history information, and • emergency/next of kin contact information.

	This information is about identifiable individuals and is "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	• In June 2015, Calgary Police Service (CPS) contacted the Organization regarding information found as part of an interprovincial identity theft investigation that led to the arrest of an individual. • The CPS informed the Organization that cellphone photographs of paper documents that appear to be from the Organization's offices (rental applications) were found on the arrested individual's computer. The individual is not known to the Organization. • The CPS believes that the personal information was compromised sometime during 2014.
Affected individuals	The incident affected twenty-seven (27) residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Retained a private investigator as well as a computer expert to investigate files, office systems and security of personal information. • Conducted a security review and implemented enhancements as necessary. • Changed contracted service providers (office cleaners and shredding companies). • Implemented new policy safeguards for protecting information and reminded employees of their privacy obligations. • Changed all employee system passwords. • Established a client portal for transmitting confidential information. • Working with law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on November 5, 2015.

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 did not specifically identify any harm that might result from this incident, but advised affected individuals to "check your accounts to determine whether or not there are any suspicious transactions associated with use of your information." In my view, the contact, identity, employment, financial and profile information at issue could be used to cause the harms of identity theft, fraud, and financial loss. 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 between the incident and the possible harm.	The Organization did not specifically assess the likelihood of harm resulting from this incident but reported that it had not received any complaints of identity theft or fraud from any of the affected individuals. In my view, there is a real risk of significant harm in this case. The incident resulted from malicious intent (unauthorized access by unknown individual associated with identity theft investigation). The Organization was unaware of the breach, and the information is believed to have been exposed for at least one year. The information may have been further disseminated and copied.

DECISION UNDER SECTION 37.1(1) OF PIPA

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

The contact, identity, employment, financial and profile information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. The incident resulted from malicious intent (unauthorized access by unknown individual associated with identity theft investigation). The Organization was unaware of the breach, and the information is believed to have been exposed for at least one year. The information may have been further disseminated and copied.

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

I understand the Organization notified the affected individuals in accordance with the Regulation on November 5, 2015. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner