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	Equicapita Income Trust (Organization)
Decision number (file number)	P2017-ND-09 (File #003673)
Date notice received by OIPC	September 6, 2016
Date Organization last provided information	September 20, 2016
Date of decision	January 6, 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 an Alberta corporation and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • name, • personal email address, • home address, • home telephone number, • personal cell phone number, • date of birth, • work title, telephone number, email address, and address, • social insurance number, • investment information (including number and dollar amount of share units held), • banking information (bank transit number and account number), • trust number (identification number specific to each investor), • divorce agreement that provides for the redemption or splitting of joint-held investments in the event of a divorce. 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	• On August 18, 2016, an employee of the Organization began to receive "Non Delivery Reports" for email(s) undeliverable to an unknown mailbox. • After an internal investigation, the Organization discovered that a corporately owned webmail account assigned to an employee of the Organization was compromised such that all incoming email received through the account between July 17, 2016 and August 16, 2016 was automatically being forwarded to an unauthorized Gmail account.
Affected individuals	Approximately 2139 individuals are affected, including 974 located in Alberta.
Steps taken to reduce risk of harm to individuals	• Initiated an investigation. • Reported the matter to Google to track down the identity of the user of the alternate account. • Reviewed all email accounts, local and web-based, to ensure no other accounts were compromised. • Offered no cost fraud protection services to affected individuals. • Conducted internal forensic review of IT security systems and enhanced IT security measures.
Steps taken to notify individuals of the incident	Notified affected individuals by email and mail during the week of September 6, 2016.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 "certain of the personal information that was disclosed through the breach, such as Social Insurance Numbers, personal addresses, and bank account information, could potentially be used to conduct identity theft." I agree with the Organization's assessment. The information at issue includes sensitive identity, financial and employment information that could be used to cause the harms of identity theft and fraud. Email addresses could be used to cause the harm of phishing. 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 reported that "the likelihood of potential harm in this particular instance is high. The Corporate Account appears to have been compromised through a purposeful attack which increases the risk that personal information may be utilized for a malicious or improper purpose."

	I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email) and the information was potentially exposed for 1 month before the incident was discovered.

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 as a result of this incident.

The information at issue includes sensitive identity, financial and employment information that could be used to cause the harms of identity theft and fraud. Email addresses could be used to cause the harm of phishing. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email) and the information was potentially exposed for 1 month before the incident was discovered.

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 that the Organization notified affected individuals by email and mail during the week of September 6, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner