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	IPC Investment Corporation (Organization)
Decision number (file number)	P2020-ND-083 (File #013226)
Date notice received by OIPC	September 5, 2019
Date Organization last provided information	September 25, 2019
Date of decision	July 24, 2020
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 all or some of the following information: • name, • residence, • telephone number, • email address, • social insurance number, • date of birth, • occupation, • employer name, • approximate income and net worth, • investment knowledge, • time horizon, • risk tolerance, • investment objective, • plan type, • account number, • fund name, and • bank account number.

	This information is about an identifiable individual 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 August 15, 2019, an advisor with the Organization prepared documents to send to a client for completion. • The advisor entered the wrong email address for the client and the message was sent to an unknown party who had a similar email address. • The breach was discovered on August 29, 2019 when the client reached out to the advisor to inquire about the documents that were to be sent by email. • The Organization was unable to determine if the email account is active or if the owner opened the attachment.
Affected individuals	The incident affected 1 individual.
Steps taken to reduce risk of harm to individuals	• Sent a request to the unknown party to request confirmation that the email was deleted. • Asked the affected individual to notify Equifax and TransUnion; to review all bank and credit card statements; to notify credit card companies and other financial institutions as well as Canada Post, utility and service provider. • Will cover the cost of credit monitoring service for the affected individual for two years. • Enhanced safeguards for affected individual's account.
Steps taken to notify individuals of the incident	The affected individual was notified verbally and sent a letter on September 5, 2019.
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 potential risk of identity theft or fraud due to the personal information records on the documents included in the email." In my view, a reasonable person would consider the contact, identity and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email address, particularly when combined with other contact, identity and financial information could be used for phishing purposes, increasing vulnerability to identity theft and fraud. 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 "There is a potential risk of harm because we do not know the owner of the email account, if the email account is active or if the owner viewed the documents, This was not a targeted attack and there was no malicious intent used to obtain the information." In my view, although the unauthorized disclosure was caused by human error, the likelihood of harm resulting from this incident is increased because the Organization did not receive a response or confirmation from the unintended recipient that the email was deleted and not copied, forwarded or otherwise distributed.

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 individual.

A reasonable person would consider the contact, identity and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email address, particularly when combined with other contact, identity and financial information could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

Although the unauthorized disclosure was caused by human error, the likelihood of harm resulting from this incident is increased because the Organization did not receive a response or confirmation from the unintended recipient that the email was deleted and not copied, forwarded or otherwise distributed.

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 individual verbally and in a letter dated on September 5, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner