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)	P2019-ND-162 (File #013315)
Date notice received by OIPC	May 24, 2019
Date Organization last provided information	May 24, 2019
Date of decision	November 20, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the 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 Organization reported the type of personal information involved was "Email address". However, as the incident involved a compromised email account, it is possible information in emails may have been involved. The Organization reported it is "…not aware if the sender was able to obtain the contents of the Advisor's emails and the email service provider has not been able to determine the cause". Email address and any information about identifiable individuals included in compromised emails are "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 2, 2019, an unauthorized sender caused a "phishing" email to be sent to email addresses from an Advisor's contact list. The phishing email was written to trick recipients into providing payment in the form of Google Play cards.

	• Responses were redirected to an alternate email and the owner of the account is not known. • Some individuals who received the communication identified it as a phishing attempt and notified the Advisor's office the same day. • The Organization's Head Office was notified of the incident on May 16, 2019.
Affected individuals	The incident affected 170 individuals.
Steps taken to reduce risk of harm to individuals	• The Advisor notified the email provider on May 2, 2019 and the email password was updated the same day that the phishing communication was issued. • The Advisor is looking at alternate email providers. • The Advisor is already using virus/malware on computers. • Individuals who provided payment to the sender will be reimbursed.
Steps taken to notify individuals of the incident	The Organization reported "A broadcast message from the Advisor was issued to warn recipients about the phishing communication. The message confirmed that the email did not come from the Advisor and to disregard." Notification occurred via "Email and the Advisor was calling clients individually after returning to Canada on or around May 10, 2019. [The Organization's] Head Office is currently preparing a formal letter to issue to affected individuals." Affected individuals were notified "May 3 and May 17".
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 "A breach of email address could result in identity theft and/or fraud through phishing and/or social engineering attempts. Although there is no direct evidence the sender obtained access to the contents of the Advisor's emails with personal information, the risk exists that information could be used to cause the harms of identity theft, fraud and/or financial loss." In my view, a reasonable person would consider that email addresses could be used for the significant harm of phishing, increasing vulnerability to identity theft and fraud. Depending on the content of emails containing personal information (that may have been compromised), other significant harms may be possible.
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: *The information currently available suggests the incident was limited to obtaining access to email addresses for the purpose of sending a phishing [sic] to lure recipients into providing payment in Google Play cards. We can confirm*

between the incident and the possible harm.	*that a risk of harm already occurred whereby two individuals did not recognize the phishing attempt and provided payment.* The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent by an unknown third party and the personal information was used to send additional phishing emails. The breach has already resulted in two incidents of fraudulent payments.

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 email addresses could be used for the significant harm of phishing, increasing vulnerability to identity theft and fraud. Depending on the content of emails containing personal information (that may have been compromised), other significant harms may be possible.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent by an unknown third party and the personal information was used to send phishing emails. The breach has already resulted in two incidents of fraudulent payments.

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 reported it was "…preparing a formal letter to issue to affected individuals." I require the Organization to confirm to my office in writing, within 10 days of the date of this decision, that affected individuals in Alberta have been notified in compliance with the Regulation.

Jill Clayton
Information and Privacy Commissioner