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	Industrial Alliance Insurance and Financial Services Inc. (Organization)
Decision number (file number)	P2020-ND-001 (File #013691)
Date notice received by OIPC	September 6, 2019
Date Organization last provided information	September 6, 2019
Date of decision	January 31, 2020
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 whose personal 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 "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue includes: • first and last name, • Social Insurance Number, • banking information, • health information, • date of birth, • address, • product information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 20, 2019, the email account of a representative of the Organization was accessed as the result of a phishing incident.

	• The hacker accessed the email box again on July 17, 2019, including all emails in the email box and the personal information in the emails. • The incident was discovered on July 17, 2019, when some of the Organization's employees received phishing e-mails and informed IT services.
Affected individuals	The incident affected 335 individuals, including 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately took steps to regain control of the compromised e-mail box, and deny access to the hacker. • Offered credit monitoring for a period of 5 years to all affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter August 23, 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 "There is however a small possibility of identity theft or fraud, which could lead to economic loss." In my view, a reasonable person would consider that the contact, identity, financial and health information at issue could be used to cause the significant harms of identity theft and fraud.
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 the likelihood of harm resulting from this incident as "Low, considering the fact that the person who took control of the e-mail box primarily intended to use it to send other malicious e-mails from the e-mail box and not to use the personal information in the contents of the box." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action). The Organization can only speculate as to the motives of the sender of the phishing email and the compromised account was used to send additional phishing emails, increasing the likelihood of identity theft or fraud resulting from the incident.
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 the contact, identity, financial and health information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action). The Organization can only speculate as to the motives of the sender of the phishing email and the compromised account was used to send additional phishing emails, increasing the likelihood of identity theft or fraud resulting from the incident.

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 individuals were notified by letter August 23, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner