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., on behalf of its wholly owned subsidiaries Industrial Alliance Securities Inc. and Investia Financial Services Inc. (the Organization)
Decision number (file number)	P2020-ND-150 (File #015689)
Date notice received by OIPC	April 16, 2020
Date Organization last provided information	April 16, 2020
Date of decision	November 20, 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 those 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 incident involved all or some of the following information about current and former employees: • name, • address, • email address, • identification card, • Social Insurance Number, • banking and financial information, • credit card information, • driver's license number, and • passport information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or around August 27, 2019, the Organization discovered that unauthorized spam messages containing malicious links had been sent internally from the email accounts of certain financial advisors. • The Organization immediately investigated and confirmed that between August 26, 2019 and September 30, 2019, the email accounts of eighteen (18) advisors were compromised because of a phishing campaign, which led to these advisors divulging their user credentials to malicious websites. • The Organization reported that there is evidence that the credentials may have been used to access the contents of these mailboxes, which contained personal information belonging to clients. • The Organization's dark net scan did not find evidence to suggest any misuse of the information.
Affected individuals	The incident affected 6,789 individuals, of which 107 are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Worked closely with cybersecurity experts. • Effected mandatory password reset across the affected environment. • Implemented two-factor authentication for the majority of advisors. • Implemented 24/7 security information event monitoring to review activity logs to detect suspicious activity. • Optimized anti-spam software and enabled an anti-phishing tool. • Implemented additional security safeguards to protect personal information, e.g. advisors now undergo additional email verification steps when accessing email remotely. • Issued a series of internal announcements to advisors regarding phishing emails and general security information. • Implemented further cyber security awareness training. • Offered credit monitoring services for a period of five (5) years paid in full by the Organization.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone beginning on April 20, 2020.

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, "Possible harms include fraud and identity theft." In my view, a reasonable person would consider the contact, financial and identity information (Social Insurance Number) at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for phishing, 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 "The results of a dark net scan undertaken by the cybersecurity forensics firm did not find evidence to suggest any misuse of the information. Consequently, we believe the risk of harm is medium to low". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party. Although the Organization reported that it has no evidence that the personal information at issue has been misused, identity theft and fraud can occur months and even years after a data breach.

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 the contact, financial and identity information (Social Insurance Number) at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party. Although the Organization reported that it has no evidence that the personal information at issue has been misused, identity theft and fraud can occur months and even years after a data breach.

I require the Organization to notify the affected individuals whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by telephone starting April 20, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner