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	PPI Management Inc. (Organization)
Decision number (file number)	P2021-ND-058 (File #016620)
Date notice received by OIPC	August 5, 2020
Date Organization last provided information	August 5, 2020
Date of decision	March 9, 2021
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 a wholly owned subsidiary of Industrial Alliance Insurance and Financial Services Inc. and 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, • date of birth, • government-issued ID, • social insurance number, and • financial 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 September 19, 2019, the Organization's IT staff discovered that unauthorized spam messages containing malicious links that harvested credentials had been sent from the email account of one (1) of its employees.

	• The incident took place between September 17, 2019 and September 19, 2019. • The Organization took immediate steps to secure the affected account, engaged external legal counsel and a third-party cybersecurity firm to investigate the incident. • The Organization's investigation confirmed that a total of seven (7) of its email accounts were likely compromised as a result of a phishing attack.
Affected individuals	The incident affected 5,117 Canadians of which eighty-seven (87) are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged a cybersecurity firm to investigate the incident and assist with containment. • Reset passwords on all affected accounts. • Removed affected computers from the network, and analyzed them before putting them back on the network or rebuilding them. • Blocked the DNS (Domain Name System) domain. • Engaged a third-party cybersecurity firm to review its incident response post-mortem. • Engaged a third-party cybersecurity firm to conduct a dark web scan. The scan did not find evidence that any personal information has been misused. • Offering all potentially affected individuals credit monitoring services for a period of five (5) years. • Provided training to employee in cybersecurity courses and to remain vigilant when it comes to their own mailbox.
Steps taken to notify individuals of the incident	The affected individuals were notified by telephone and by letter beginning August 7, 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 or identity theft." In my view, a reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss.

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 (deliberate intrusion). The lack of evidence to date to suggest any misuse of the information is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, the intruder had access to the information for approximately three (3) days.

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 identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. 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 (deliberate intrusion). The lack of evidence to date to suggest any misuse of the information is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, the intruder had access to the information for approximately three (3) days.

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 the Organization notified affected individuals by telephone and by letter beginning August 7, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner