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	Richardson Wealth Limited (formerly Richardson GMP Limited) (Organization)
Decision number (file number)	P2021-ND-127 (File #017142)
Date notice received by OIPC	August 12, 2020
Date Organization last provided information	August 12, 2020
Date of decision	May 12, 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 individual 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 operates in Alberta 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: • full name, • account number(s) and account types, and • other financial institution information and account types held. 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 1, 2020, a privacy breach occurred due to a successful phishing attempt where an employee clicked on a link in an email sent by a malicious party and entered their credentials. • The malicious party accessed the employee's email inbox. • Evidence suggests that seven (7) emails were viewed, resulting in the disclosure of personal information of nine (9) clients, one (1) of which is a client at a Calgary branch.

Affected individuals	The incident affected 9 individuals, including 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Reset the compromised employee's password and disabled their email and network access. • Contained the incident. • Blocked the phishing scheme preventing future attempts. • Issued new account numbers. • Offered credit-monitoring services in which the cost will be covered by the organization. • Monitoring client accounts for unusual or suspicious activity. • Updating Privacy Breach Policy and Procedures. • Reminded all employees to be aware and reiterated the importance of being vigilant when responding to emails, texts and phone calls requesting personal information.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 2, 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 the possible harms that may occur as a result of the breach include "Fraud, security risk, financial loss and phishing". I agree with the Organization's assessment. A reasonable person would consider that the contact and financial information at issue could be used for the purposes of identity theft and fraud. Email address 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, *There is a low risk of ongoing Privacy Breach or further exposure of Personal Information given that the threat was contained and anti-malware firms have blacklisted this phishing scheme, preventing future attempts. The employee whose inbox was compromised had their network password reset. The malicious party no longer has access to the employee's account. However, the personal information disclosed can be used for fraudulant [sic] and harmful purposes like identity theft, financial loss, risk of fraud and phishing. Although the incident has been contained, the malicious party and their intentions on using the disclosed information are unknown to the firm. As such, we must assume that there is a high risk of unforeseeable harm to the clients and handle this incident with a higher standard of client care and remediation.*

	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 (phishing). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the compromised information were to be used for fraudulent purposes.

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 and financial information at issue could be used for the purposes of identity theft and fraud. Email address 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 (phishing). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the compromised information were to be used for fraudulent purposes.

I require the Organization to notify the affected individual 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 letter on July 2, 2020 in accordance with the Regulations. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner