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 GMP Ltd. (Organization)
Decision number (file number)	P2021-ND-015 (File #016469)
Date notice received by OIPC	September 13, 2019
Date Organization last provided information	September 13, 2019
Date of decision	February 16, 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 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: • name, and • private investment information (market value, cost base value, status, income generated, and total gain/loss in dollars and percentage). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• In June 28, 2019, an administrative error caused an investment update document to be inadvertently mailed to out of date addresses. The addresses were former employment addresses for now retired clients. • The breach was discovered on July 2, 2019 when an unintended recipient reported opening and subsequently shredding the mailing.

Affected individuals	The incident affected 12 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Updated addresses in the contact management system that did not match the client's official address on the Organization's internal system. • Reviewed and reconciled mailing addresses within systems.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally on or about July 5, 2019 and by letter on or about August 22, 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, *A* [sic] *unauthorized person may use the compromised personal and account information to gather additional confidential information through social engineering or another means. On its own, the compromised information has limited potential to cause harm to the client.* 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 and/or fraud. In addition, because the Organization reported the compromised information may be used to "gather additional confidential information through social engineering or other means", I accept there is a potential for additional harm in this case.
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 resulting harm is limited. The unintended recipient(s) have limited information such as the client's name and the private Investment portion of the client's portfolio. Account numbers … and social insurance numbers were not disclosed.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased because it was caused by human error. However, it is not clear whether the Organization requested that the unintended recipients securely shred or return the letter or whether it confirmed the information was not copied, forwarded or otherwise distributed.
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 and/or fraud. In addition, because the Organization reported the compromised information may be used to "gather additional confidential information through social engineering or other means", I accept there is a potential for additional harm in this case.

The likelihood of harm resulting from this incident is decreased because it was caused by human error. However, it is not clear whether the Organization requested that the unintended recipients securely shred or return the letter or whether it confirmed the information was not copied, forwarded or otherwise distributed.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals verbally on or about July 5, 2019 and by letter on or about August 22, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner