



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-104 (File #013051)
Date notice received by OIPC	April 16, 2019
Date Organization last provided information	April 16, 2019
Date of decision	March 31, 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 <i>Personal Information Protection Act</i> (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”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• address,• account holdings within various accounts in the clients' names,• market value of accounts, and• account and client numbers. <p>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.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	

<p>Description of incident</p>	<ul style="list-style-type: none"> • On January 7, 2019, an Investment Advisor with the Organization received an email from a client requesting copies of the client’s current investment portfolio statement and account balances. • The Advisor responded the same day, but attached the wrong clients’ Portfolio Evaluations in error. • On January 14, 2019, the original client advised the Organization that she was a victim of fraud, where it appears that a fraudster hacked and used the email address to correspond with the Organization. • The breach was discovered on March 14, 2019 during the Organization’s review of the circumstances associated with the fraud attempt.
<p>Affected individuals</p>	<p>The incident affected 3 individuals in Alberta.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • Restricted withdrawals and enhanced security for affected accounts, and changing account numbers for affected individuals. • Ceased to use the compromised email address. • Reported the incident to other affected parties (including relevant bank institutions). • Encouraging clients to use online account access so that information can be sent to them via secure channel.
<p>Steps taken to notify individuals of the incident</p>	<p>Affected individuals were notified by letter on April 3, 2019.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<p>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.</p>	<p>The Organization reported:</p> <p style="text-align: center;"><i>The use of the personal information would be limited as the information that the fraudster can reasonable [sic] use only includes the client's name, address and [Organization] account numbers (which has [sic] since been changed).</i></p> <p>The Organization also said “However, there is a high likelihood that if the fraudster is able to manipulate or misuse any of the information, they will”.</p> <p>In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause significant harms such as identity theft and fraud.</p>

<p>Real Risk</p> <p>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.</p>	<p>The Organization reported “The unauthorized recipient(s) are not trusted individuals and would likely seek to misuse the information if given the opportunity”.</p> <p>In my view, a reasonable person would consider that the circumstances of this breach give rise to a real risk of significant harm to the individuals. The contact and financial information was disclosed in error, likely to an individual with malicious intent. The Organization did not report that the information was recovered or that the perpetrators were apprehended.</p>
---	--

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 to cause significant harms such as identity theft and fraud. The contact and financial information was disclosed in error, likely to an individual with malicious intent. The Organization did not report that the information was recovered or that the perpetrators were apprehended.

The Organization is required 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 affected individuals were notified by letter on April 3, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner