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 (Organization) |
| **Decision number (file number)** | P2021-ND-212 (File #019617) |
| **Date notice received by OIPC** | February 24, 2021 |
| **Date Organization last provided information** | February 24, 2021 |
| **Date of decision** | November 1, 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 an "organization" as defined in section 1(1)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The Organization reported the incident involved some or all of the following information:<br><br>• full name,<br>• account number,<br>• social insurance number,<br>• client ID,<br>• date of birth,<br>• address,<br>• telephone number,<br>• email address,<br>• employment information,<br>• name of spouse and employment information,<br>• income, net worth, account type,<br>• driver's license number (client and spouse's),<br>• credit report and spouse's credit report,<br>• other financial institution account number/type/balances/transit number/institution number,<br>• beneficiary information, and<br>• details of one transaction. |

| | |
|---|---|
| | 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 January 28, 2021, an employee with the Organization clicked on a link in a phishing email, which gave unauthorized actors her credentials and access to the employee's email box.<br>• The Organization conducted a review and determined that there were 16 emails that contained sensitive personal information that could potentially create a risk harm for five individuals in Alberta.<br>• The Organization reported that it is unknown whether the unauthorized actors actually read the emails and their attachments. |
| **Affected individuals** | The incident affected 5 Alberta residents. |
| **Steps taken to reduce risk of harm to individuals** | • Revoked multifactor authentication sessions and reset the employee's email account password.<br>• Offered new account numbers for clients whose account numbers and client IDs may have been disclosed.<br>• Offered credit monitoring services for the clients whose SINs were included in the emails.<br>• Advised individuals whose account numbers at another financial institution were included in the emails that they may wish to contact their other financial institution, in case they would also like to take preventative measures, such as changing account numbers.<br>• Will monitor client accounts for unusual or suspicious activity.<br>• Required all employees to complete an annual training course on the privacy policy and procedures.<br>• Required all employees to complete the annual training course at the end of December 2020.<br>• Implemented a new email banner that informs employees if the email they received is from an external party. |

| | |
|---|---|
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on February 11, 2021. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>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,<br><br>*The information can be used for fraud, phishing and identity theft or cause financial loss.*<br><br>I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, financial and employment information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms. |
| **Real Risk**<br>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:<br><br>*We have determined that 131 emails were clicked on. However, the bad actor and their intentions on using the potentially disclosed information are unknown to the firm. Out of an abundance of caution, we will assume that the personal information was disclosed and handle this incident with a higher standard of client care and remediation. Even if we assume all of the client personal information was disclosed, the information that may have been disclosed cannot be used elsewhere and internal controls are in place to prevent the bad actor from successfully making a transaction. For example: Fraud Prevention Form requires that IAs confirm all instructions with the client directly before executing them. Therefore, we believe there is no real risk of significant (sic) harm to our clients.*<br><br>In its notification to affected individuals, the Organization said…<br><br>*...we suggest that you notify your other financial institution regarding the incident. To protect yourself against the identity theft, we suggest that you review your bank accounts for any unusual activity. You may also wish to explore credit monitoring services, … As a matter of best practice, please be cautious when clicking on links sent via email or responding to emails, texts or phone calls requesting for personal information and to check the legitimacy of the sender even when it comes from a known individual or company that you trust.*<br><br>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, 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 information accessed were to be used for fraudulent purposes, for example. |

**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, identity, financial and employment information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email addresses could be used for the purposes of 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 (deliberate intrusion, 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 information accessed were to be used for fraudulent purposes, for example.

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 the affected individuals by letter on February 11, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner