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	Raymond James Ltd. (Organization)
Decision number (file number)	P2022-ND-010 (File #022225)
Date notice received by OIPC	July 15, 2021
Date Organization last provided information	July 15, 2021
Date of decision	March 27, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those 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: • contents of cover letters and resumes (name, address, phone number, and job history/experience), • tokenized email address (for applicants that did not respond to the phishing attempt. The tokenized email address is the masked Indeed email address, not the applicant's personal email address), • personal email address (for applicants that responded directly to the phishing attempt), and • copy of a passport (for one individual). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's website and/or application. The Organization reported, "However, as responses were sent directly by the affected individuals to the adversary, outside of the RJL Employer Portal and outside of the Indeed platform, neither

	RJL nor Indeed has specific details on the actual information a particular affected individual may have sent."
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On March 24, 2021, an unknown adversary gained access to the Organization's Employer Portal on the Indeed.com (Indeed) job-posting platform. • Indeed was notified immediately. Access to the Organization's Employer Account was frozen by Indeed. Password changes were implemented by the Organization. • The adversary had access to the Organization's Employer Portal for approximately 2 hours and 15 minutes on March 24, 2021. • During that period of compromise, the adversary sent out the first batch of phishing emails to the Indeed tokenized emails of 3,818 applicants on the Portal. • The phishing email sent by the adversary requested the applicants to send their cover letters and resumes to the adversary's email address of raymond_james_ltd@outlook.com. • The adversary also scraped and exported those tokenized emails and used them outside of the Organization's Employer Portal on March 25, 2021 to directly send a second batch of phishing emails to those applicants. • In addition, with access to the Organization's Indeed portal messaging mailbox communication history / application submissions, the adversary could have allowed harvested CVs/resumes of job applicants. • Indeed was unable to provide logs to confirm if applications or mailbox communication history was accessed. The Organization does not utilize the Indeed mailbox for communication and instead uses its own email system. • Ninety-six (96) individuals emailed the Organization to indicate that they had sent personal information to the adversary in response to that phishing email. However, only 18 of those 96 provided the Organization with appropriate evidence of harm. • The root cause was an Organization password, which did not follow the Organization's password requirements/ standards. There was also a lack of multi-factor authentication.
Affected individuals	The incident affected eighteen (18) individuals. Three were international individuals and fifteen (15) were Canadians, including two (2) individuals whose information was collected in Alberta.

Steps taken to reduce risk of harm to individuals	Indeed: • Notified affected individuals. • Worked to identify and prevent potentially fraudulent activity on the account. • Investigated and disabled the Organization's accounts before reinstatement. • Confirmed the incident was an isolated case. The point of access was at the Organization's end and was not due to an entry point or weakness at the Indeed end. • Deleted the tokenized email addresses used by the adversary to prevent future use. Organization: • Investigated its Employer Portal on Indeed. • Changed and followed its current standard for passwords to its Employer Portal on the Indeed site and all other similar job portals. • Added two-factor authentication. • Checked to ensure no false job postings on Indeed and other job portals. • Updated its careers page and job postings on its public website to include a warning to users of potential Job Scam Phishing. • Requested Microsoft take down adversary's phishing email address. • Attempted to identify the adversary but was unsuccessful. • Offered comprehensive credit monitoring and identity theft protection plan for a 12 month period at no cost to affected individuals who provided responses to the adversary and that contacted the Organization and provided appropriate evidence of potential harm.
Steps taken to notify individuals of the incident	At the Organization's request, Indeed notified affected individuals on March 26, 2021 and April 12, 2021.
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 include fraud and identity theft.* In my view, a reasonable person would consider the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Confirmed valid credentials could be used to compromise online accounts. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms. Because the Organization cannot identify all the personal information that was accessed by

	the unknown adversary, it is not clear what other possible harms may exist.
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, *We were unable to identify the adversary but based on the nature of the attack and the information available to the adversary, we assume that there was malicious intent and a likelihood that the information could be used for malicious purposes. At the same time, the number of individuals who responded to the phishing attempt, based on their outreach to us, was relatively small. Information that was obtained was for the most part not sensitive information like SIN, credit card information, etc. However one individual from Cameroon sent a copy of his passport. We have not been made aware of any specific harms experienced by any of the affected individuals at this point.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident is the result of malicious actions by an unknown adversary. In some cases, the phishing attempt by the adversary was successful. Although the Organization reported that it has *"not been made aware of any specific harms experiences by any of the affected individuals at this point*", I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach.

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 the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Confirmed valid credentials could be used to compromise online accounts. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms. Because the Organization cannot identify all the personal information that was accessed by the unknown adversary, it is not clear what other possible harms may exist.

The likelihood of harm resulting from this incident is increased because the incident is the result of malicious actions by an unknown adversary. In some cases, the phishing attempt by the adversary was successful. Although the Organization reported that it has "not been made aware of any specific harms experiences by any of the affected individuals at this point", I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach.

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 that Indeed notified affected individuals on the Organization's behalf on March 26, 2021 and April 12, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance