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** | CPA Western School of Business (Organization) |
| **Decision number (file number)** | P2020-ND-109 (File #015824) |
| **Date notice received by OIPC** | May 12, 2020 |
| **Date Organization last provided information** | May 27, 2020 |
| **Date of decision** | September 24, 2020 |
| **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 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:<br>• name,<br>• address,<br>• telephone number,<br>• email address,<br>• cover letter content,<br>• work history,<br>• other job offers,<br>• academic transcript, and<br>• academic degree.<br><br>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** | • An employee with the Organization clicked on a phishing email, which created a rule that auto-forwarded incoming email messages to an unknown third-party, moved the messages to a rarely-used Outlook folder in the employee's Outlook, and deleted information from the sent folder without the staff member's knowledge.<br>• The "hacked" emails sent to the employee's work email account were from applicants responding to fabricated job postings that the hacker created after having opened a fraudulent account for the Organization on Indeed.com.<br>• A total of 364 messages were forwarded from the employee's work email account between April 17 and April 30; a review found that the emails included the personal information of 22 individuals. |
| **Affected individuals** | The incident affected 22 individuals. |
| **Steps taken to reduce risk of harm to individuals** | • Offered six months of Equifax Pro Monitoring to residents of Canada.<br>• Disabled the functionality that allowed the messages to be auto-forwarded on all the Organization's email accounts.<br>• Changed the employee's network password. |
| **Steps taken to notify individuals of the incident** | The Organization reported that "Because Indeed creates an alias for applicants, it is currently not possible to notify most of the individuals who applied for the job posting and whose emails were auto-forwarded; however, some individuals included attachments that contained their email addresses and they were notified on May 12, 2020".<br><br>The Organization was able to notify 16 of the 22 individuals directly and posted a notice on its website for 30 days. |
| **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 that "The information could be used in future social engineering attacks on the people who applied for the jobs."<br><br>In my view, a reasonable person would consider that the contact employment and education information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all 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 that "Given the collection and disclosure was malicious, there is considerable risk this information was collected for all applicants to be used in future malicious acts."<br><br>I agree with the Organization's assessment. A reasonable person would consider the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (phishing and email forwarding rule). It appears the email account was exposed for approximately 13 days. |

**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 employment and education information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (phishing and email forwarding rule). It appears the email account was exposed for approximately 13 days.

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).

Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…" , although section 19.1(2) says "… the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

In this case, the Organization reported that direct notification would not be possible for 6 of the affected individuals because it did not have contact information. However, the Organization published a notice on its website (https://www.cpawsb.ca/about-cpawsb/privacy-breach) with the contact information of the privacy office for individuals seeking additional information regarding the incident.

Given the Organization's submissions, I accept that indirect or substitute notice as described by the Organization is reasonable in this case, where the Organization is unable to contact affected individuals directly.

Jill Clayton
Information and Privacy Commissioner