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	Centaur Products Inc. (Organization)
Decision number (file number)	P2021-ND-307 (File #019004)
Date notice received by OIPC	January 14, 2021
Date Organization last provided information	January 14, 2021
Date of decision	March 3, 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 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 specializes in project management, provision, installation and servicing of a wide range of sport-related construction products. The Organization has regional offices in British Columbia, Alberta, Ontario and Nova Scotia. 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 known personal information subject to the breach is the Indeed auto-generated email address alias of the two individuals to whom emails were sent from the Breached Account. At this time, Centaur is not aware of breach of any other personal information that may have been accessible from the Breached Account's email. Centaur did not receive any responses or personal information from the two affected individuals to whom the emails were sent from the Breached Account by the malicious actor(s).* *The Breached Account was accessible and/or accessed for two days on December 21 and 22, 2020. The Breached Account contained approximately 51,000 emails. A keyword search by the third party IT company of the emails in the Breached Account revealed the following:*

	There were 52 emails that contained keywords which related to Personal Information relating "Social Insurance Number" or "SIN". *Furthermore, during the investigation, the Breached Account was searched using specific target words. There were about 2,959 emails that contained keywords related to Financial Information including: credit card, Visa, Mastercard, Amex, Paypal, account number, TD, CIBC, RBC, bank* *The IT company also included the specific note that the keyword searches did not confirm the e-mails contained financial or personal information. In fact, on e-mails which were spot checked, it was determined that revealed that no personal or financial information was found or listed in the email.* To the extent this information is about identifiable individuals, it 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 December 21 and 22, 2020, malicious actor(s) accessed an employee email account and used it to create a fictitious account and post a job for a receptionist on an employment recruitment site. • The breach was discovered when an acquaintance of a staff member inquired about the job posting. On December 22, 2020, the Organization determined that it was not a valid job posting. • On December 22, 2020, the malicious actor(s) also sent emails from the breached email account to two individuals with malicious links (a link created with the purpose of promoting scams, attacks and frauds) requesting personal information. • The Organization reported that it does not know how the account was accessed. Based on its investigation, only the emails and documents within the breached email account would have been accessible. • The Organization did not receive responses or personal information from the two affected individuals to whom the emails were sent from the breached account.

Affected individuals	The incident is known to have affected two individuals. The Organization reported the total number of unique email addresses saved on the breached account that could have been accessed is approximately 2,400.
Steps taken to reduce risk of harm to individuals	• Notified the recruitment site of the fraudulent activity. The posting was flagged as fraudulent and removed. The account was also locked to prevent further use. • Reset the email account password, temporarily locked the account and verified no forwarding rules were in place to allow the malicious actor(s) to still communicate with the individuals. • Checked for unauthorized access to file servers and checked all network devices for virus/malware/trojans etc. • Adjusted internal policies to minimize the occurrence of specific information being sent via email. • Reviewing a short-term implementation of multi-factor authentication.
Steps taken to notify individuals of the incident	Affected individuals were notified by email between December 23, 2020 and January 8, 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 harms that could result from the incident as "Potential loss of personal information, including names, address, financial information." In my view, a reasonable person would consider that the information at issue in this case could be used to cause the harms of identity theft, fraud and/or financial loss. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.
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: *Harm from breach seems unlikely. It was caught quickly and direct notifications went out quickly. Spot checking user e-mails did not uncover any personal or financial information.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (spoofing email) by an unknown third party and it appears the personal information was used to send fraudulent emails, with the purpose of obtaining information. The Organization cannot rule out that approximately 2400 email addresses could have been accessed during the two-day period the information may have been available.

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 information at issue in this case could be used to cause the harms of identity theft, fraud and/or financial loss. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (spoofing email) by an unknown third party and it appears the personal information was used to send fraudulent emails, with the purpose of obtaining information. The Organization cannot rule out that approximately 2400 email addresses could have been accessed during the two-day period the information may have been available. 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 email between December 23, 2020 and January 8, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner