Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organizations	CDI Education (Alberta) Inc. o/a CDI College – Business Technology Healthcare, Reeves Education (Alberta) Inc. o/a Reeves College, and VCAD Education (Alberta) Inc. o/a VCAD – Visual College of Art and Design (collectively, the "Organizations")
Decision number (file number)	P2023 - ND-020 (File #023823)
Information received by OIPC	In November 2021, a member of the media contacted my office and stated that the Organizations may have suffered a loss, an unauthorized access to, or an unauthorized disclosure of personal information under the Organizations' control. On November 12, 2021, my office contacted CDI College. On November 15, 2021, the Organizations, through legal counsel, submitted a "*Voluntary Report of Security Incidents*" to my office. It stated, "*Once the investigation is complete, we will fulfill any notification obligations pursuant to applicable law (including notifying impacted individuals and submitting a report to your office if our investigation reveals a privacy breach).*" My office followed up with legal counsel in May 2023 about the voluntary report. On May 19, 2023, legal counsel reported, "*Following the voluntary report, our client completed their investigation and did not proceed with a breach report or with notifying the affected individuals directly*." On September 18, 2023, the Organizations' legal counsel said: "*At the time, there was no hard evidence that personal information had been compromised and based on this initial assessment, no report was filed with your office.*" My office did not receive a notice from the Organizations under section 34.1 of the *Personal Information Protection Act* (PIPA).
Date Organization last provided information	September 18, 2023
Date of decision	November 20, 2023
Summary of decision	Section 34.1(1) of PIPA states "An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the

	loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure." Pursuant to section 37.1 (1) of PIPA, "Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure ... " Based on information provided by the Organizations in November 2021, and by their legal counsel on May 19, June 22, and September 18, 2023, I have determined that a reasonable person would consider that there exists a real risk of significant harm to individuals as a result of the unauthorized access to personal information in this case. As such, I require the Organizations 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 Organizations operate private, for-profit career colleges in Alberta. The Organizations each meet the definition of "organization" under section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	On June 23, 2023, at the request of my office, the Organizations reported that the incident involved some or all of the following information: • Student IDs & Academic Records • First Names, Last Names • Date of Birth • Home addresses • Phone numbers • Email addresses • SIN numbers • Government issued photo ID • Bank account information • Student loan/grant information • Credit card information

	• Patient x-rays and related self-disclosed medical conditions (but not medical charts), for dental patients only. The CDI College and VCAD websites state that, in addition to the above, some or all of the following information was also involved in the incident: • BC identity card • Permanent residence card • Driver's license • Employees only - health benefits information • Employees only - tax credit information 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 November 14 and November 15, 2021, legal counsel confirmed the Organizations were the subject of a ransomware attack. • On October 31 and November 4, 2021, the Organizations discovered that certain of their systems had been encrypted. • The incidents did not impact the Organizations' critical business operations. • Having received no further information from the Organizations, my office asked the Organizations' legal counsel on May 9, 2023, if the Organizations could confirm whether their investigation into the incidents was complete and whether the Organizations notified affected individuals. • The Organizations reported the investigation was complete on or around May 18, 2022. • On September 18, 2023, the Organizations reported, "*At the time, there was no hard evidence that personal information had been compromised and based on this initial assessment, no report was filed with your office.*" • The Organizations reported affected individuals were notified as described below.
Affected individuals	The Organizations did not provide the number of affected individuals.
Steps taken to reduce risk of harm to individuals	When the Organizations first provided information in November 2021, the Organizations said the following steps were taken:

	- Took immediate action to contain and isolate any threat by proactively disconnecting affected systems from its network. - Engaged a team of third-party experts to assist in an investigation and notified law enforcement. - Engaged in ongoing investigation that involves a thorough review and validation of potentially affected systems and data, including personal information. - Safe restoration from these back-ups (with the assistance of the third-party experts) in progress.
Steps taken to notify individuals of the incident	On May 19, 2023, the Organizations' legal counsel reported, "…*our client completed their investigation and did not proceed with a breach report or with notifying the affected individuals directly*." However, on September 18, 2023, the Organizations reported, "…*notifications were sent to all available staff and student email addresses in our system at that time. CDI, Reeves, VCAD websites posted indirect notifications."* <u>Students</u> On November 24, 2021, affected students with known email addresses were sent an email by CDI College about the incidents. A sample of this email was provided to my office on May 19, August 28, and September 18, 2023. <u>Employees</u> On November 12, and November 24, 2021, affected employees located in Alberta were sent emails about the incidents by CDI Campus Support. A sample of this email was provided to my office on May 19, August 28, and September 18, 2023. The notice is called "*Details on the recent cybersecurity incident*" and states that, "*Any individual impacted by this situation has been notified directly. Information regarding the information concerned and steps to subscribe to free credit monitoring services were provided. At this time, we are not aware of any misuse of personal information."* The Organizations also provided an email called, "*Announcement from Campus Support to all employees / Communiqué du Collège CDI à tous les employés"* that was sent out in November 2021. The Announcement email says that the Organizations were *"…currently investigating a cybersecurity incident. We have identified that our system was targeted through sophisticated means and we are in the process of evaluating the impact of this event."*

	It is unclear whether the "*Details on the recent cybersecurity incident*" is the only notification provided to the Organizations' employees given that it says that affected individuals have already been notified. <u>Website postings</u> The Organizations posted notices on their websites about the incidents. The content of the postings was provided to my office on May 19 and September 18, 2023. It is not known the dates these notices were posted. <u>Dental Patients</u> Based on what the Organizations have reported to my office to date, it appears dental patients were not directly notified. The Organizations' reported, *"We are unaware to date of any patient, student or employee being affected by the breach. Patients would have access to the notification posted on the CDI & Reeves website."*
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 Organizations did not specifically identify any harm that might result from this incident. However, the sample notification provided to students stated, *…Should the investigation reveal that any personal information was subject to a privacy breach, we will notify directly any person affected by the situation and offer them free credit protection services.* *In the meantime, we encourage students to remain vigilant about unsolicited requests for financial or other personal information and any unauthorized transactions.* The sample notice to employees stated, *Any person affected is being notified and offered free credit protection services.* There was no information provided that dental patients were given any direct notice other than what the Organizations stated above concerning CDI and Reeves website postings. In my view, a reasonable person would consider the contact, identity, and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Medical information is sensitive information. The medical information of dental patients could be used to cause

	embarrassment, hurt and/or humiliation. These are all 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.	Legal counsel for the Organizations stated in correspondence with my office dated September 18, 2023: *We are unaware of any individuals who were affected by this incident. As noted above, notifications were sent to all available staff and student email addresses in our system at that time. CDI, Reeves, VCAD websites posted indirect notifications.* The Organizations' email to their students stated, *We are not aware of any misuse of personal information at this stage.* The Organizations' email to their employees stated, *At this time, we are not aware of any misuse of personal information. However, we do encourage everyone to remain vigilant about unsolicited requests for financial or other personal information, and any unauthorized transactions.* On September 18, 2023, the Organization reported, "*At the time, there was no hard evidence that personal information had been compromised and based on this initial assessment, no report was filed with your office."* The Organizations website notices state that unauthorized third parties gained access to IT systems and to some of the personal information that was stored on servers. There have been instances where an organization subject to a ransomware incident has provided evidence to my office to demonstrate an incident did not result in an unauthorized access to or disclosure of personal information. The Organizations in this case, however, did not provide such evidence. Therefore, 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 (intrusion, ransomware). The lack of evidence that the personal information has been misused is not a mitigating factor, as identity theft, fraud and financial loss can occur months and even years after a data breach. The threshold is "real risk of significant harm." It is not, as indicated by the Organizations' submission, lack of awareness of any actual misuse of the information.

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. The contact, identity, and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Medical information could be used to cause embarrassment, hurt and/or humiliation. These are all 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 (intrusion, ransomware). The lack of evidence that the personal information has been misused is not a mitigating factor, as identity theft, fraud and financial loss can occur months and even years after a data breach. The threshold is "real risk of significant harm." It is not, as indicated by the Organizations' submission, lack of awareness of any actual misuse of the information. It is unclear whether Reeves College and VCAD provided direct notification to their students as the samples of emails appear to come from one of the Organizations, for example "CDI College." I am relying on the legal counsel's submission made on September 18, 2023, that the Organizations directly notified students and employees at the time of the incidents if they had the email addresses. However, the sample emails of the notices to students and employees provided do not contain all of the required elements of a notice under section 19.1 of the PIPA Regulations. The notifications are missing a description of the personal information involved. The Organization did not provide direct notification to dental patients. **The Organizations who had control of the personal information of dental patients are required to confirm to my office, within fourteen (14) days of the date of this decision that those affected individuals have been notified of this incident in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and to provide my office with a copy of the notification.** **The Organizations are required to confirm to my office, within fourteen (14) days of the date of this decision, that the Organizations have re-notified affected students and employees for whom they have contact information in accordance with the requirements of the PIPA Regulation, including a description of what personal information was affected in the incident as required in section 19.1(1)(b)(iii) of the 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." Legal counsel provided links to website notices for the Organizations and reported, "*Following the voluntary report, our client completed their investigation and did not proceed with a breach report or*	

with notifying the affected individuals directly…The following indirect notifications were however proactively made, (a) in order to mitigate the potential impact of the incident, and (b) because this was most efficient given the lack of availability of current contact information for a significant number of stakeholders in Alberta.

I accept the Organizations' submission that it is reasonable in the circumstances to indirectly notify the remaining affected students and employees whose contact information is not readily available by the means of a posting on their websites.

The website notices for CDI College and VCAD as viewed on the website or provided by legal counsel meet the requirements of s.19.1 of the Regulations for indirect notification of affected students and employees whose contact information is not readily available.

However, the Reeves College website notice did not include the date on which or time period during which the loss or unauthorized access or disclosure occurred or a description of what personal information was affected in the incident as required in section 19.1(1)(b)(ii) and section 19.1(1)(b)(iii) of the Regulation.

Reeves College is required to confirm to my Office, within fourteen (14) days of the date of this decision, that any indirect notices posted on their websites meet the requirements of the PIPA Regulation, including the date on which or time period during which the loss or unauthorized access or disclosure occurred and a description of what personal information affected in the incident as required in section 19.1(1)(b)(ii) and section 19.1(1)(b)(iii) of the Regulation.

Cara-Lynn Stelmack
Assistant Commissioner, Case Management