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	Chartered Professional Accountants of Canada (the Organization)
Decision number (file number)	P2020-ND-098 (File #015962)
Date notice received by OIPC	June 3, 2020
Date Organization last provided information	July 13, 2020
Date of decision	September 3, 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 the individuals 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 incident involved all or some of the following information: • name, • address, • email address(es), • employer name and job title, • CPA Canada membership number, • membership type and membership status, and • some partial credit card numbers and expiry dates. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the email addresses of the affected individuals may include business email addresses and may qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for

	the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized disclosure of the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies. In some cases, the Organization said the password used to access "My Account" on its website and/or credit card numbers may have been affected. However, the Organization confirmed that this information was encrypted. For some individuals, the Organization said the password responses supplied for resetting passwords to "My Account" were also affected, e.g. favourite colour, mother's' maiden name, name of pet, name of the city of birth and/or the name of high school. The Organization reported that this information cannot be used to access the Organization's website account because its current password reset process does not use this information.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• From April 20 to 24, 2020, the Organization discovered a potential security incident and possible phishing activity relating to its website and email addresses of its members. • The Organization learned that unauthorized parties accessed certain information held by the Organization through an attack against its website between November 30, 2019 and May 1, 2020. • The Organization collects a range of general contact, professional and related profile information in the course of its interactions with current and former members and other individuals, including in relation to its magazine, the "My Account" section of its website and other programs and activities.
Affected individuals	The incident affected 329,640 individuals, of which 38,913 are in Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately commenced an investigation. • Notified the Canadian Anti-Fraud Centre. • Issued a notification to its members and on its website.

	• Secured its systems and conducted an analysis to determine what information may have been affected. • Encouraged individuals to review whether other services they use rely on password clues and to take action accordingly. • Notified Privacy Commissioners of Alberta, British Columbia, Quebec and Canada, and relevant authorities in the USA. • Enhanced monitoring and prevention measures and implementing additional measures to further enhance its cyber security program to help reduce the risk of such incidents in future.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on June 3, 2020. Individuals whose email address bounced back or who did not have an email address were notified by regular mail.
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 that the "CPA has identified a potential risk of harm of phishing in relation to this incident." I agree with the Organization's assessment. A reasonable person would consider the contact information and membership number, along with email address, could be used for the purposes of phishing, increasing the affected individuals' 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 that for passwords used to access "My Account" on its website and/or credit card numbers, it "confirmed that this information was encrypted and is not considered to present a risk of harm." As well, the Organization reported that the password recovery "information cannot be used to access the …website account because [the Organization's] current password reset process does not use this information. This information is considered to present a low risk of harm." In my view, a reasonable person would consider that for the remainder of the information, 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). Further, the information may have been exposed for approximately five (5) months.
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 resulting from this incident.	

A reasonable person would consider the contact information and membership number, along with email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms. For the remainder of the information, 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). Further, the information may have been exposed for approximately five (5) months.

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 on June 3, 2020, in accordance with the Regulation. Individuals whose email address bounced back or who did not have an email address were notified by regular mail. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner