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	The Certified General Accountants' Association of Alberta (Organization)
Decision number (file number)	P2013-ND-41 (File #P2482)
Date notice received by OIPC	October 22, 2013
Date Organization last provided information	November 7, 2013
Date of decision	December 2, 2013
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 is incorporated by Schedule 2, section 2 of the Alberta *Regulated Accounting Profession Act* and is registered in Alberta. The Organization is a "professional regulatory organization" as defined by section (1)(1)(k.2) of PIPA. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • job title, • phone number, • email address, • highest level of education category, • age group range, • years in finance, • how the registrant learned about the event,

	• events of interest to the registrant, and • IP address. The information listed above is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On July 30, 2013, the Organization discovered that one of its web servers was sending out mass emails not authorized by the Organization. • The server is located in Calgary, Alberta. • A vulnerability in software used by the Organization to create marketing websites on the server was exploited. As a result, downloaded malware caused spam email to be sent from the server to email addresses unrelated to the Organization. • The compromised web server contained the personal information of individuals who registered for a career expo with the Organization. • The Organization could not confirm if the personal information was accessed or disclosed as a result of the malware. However, the malware had the potential for the unauthorized user to perform additional actions on the server. Therefore, the Organization reported there may have been unauthorized access to personal information on the server that the Organization is unable to detect.
Affected individuals	Approximately 4200 individuals who registered with the Organization for a career expo.
Steps taken to reduce risk of harm to individuals	The server and email function were shut down on July 30, 2013.
Steps taken to notify individuals of the incident	The Organization has not notified any affected individuals.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those affected individuals as a result of the incident. The harm must also be	The Organization identified that the affected individuals may be at risk for phishing due to the number of emails and contact information involved. In my view, the personal information involved is of low sensitivity. However, due to the nature of the intrusion and the

"significant." It must be important, meaningful, and with non-trivial consequences or effects.	significant number of email addresses, addresses and phone numbers involved, I agree with the Organization that the affected individuals may be at risk for phishing. In my view, this is a significant harm.
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 since the intrusion used the server to send spam email to email addresses unrelated to the Organization, the possibility that the malware collected personal information from the compromised web server as a secondary objective to use for another similar event could not be ruled out. In my view, the likelihood of harm resulting from this incident is increased because of the nature of the malware and the unauthorized access. A significant number of email addresses and contact information are involved in this incident. In my view, these factors increase the likelihood of phishing as a result of this incident.

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 incident involved the installation of malware on the server. The malware sent spam email to unrelated email addresses using the Organization server. The Organization submitted that due to the nature of the malware, the possibility could not be ruled out that the malware collected personal information during the incident that could be used for phishing.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and notify me in writing it has done so on or before December 18, 2013.

Jill Clayton
Information and Privacy Commissioner