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	Alberta Hospitality Safety Association (Organization)
Decision number (file number)	P2018-ND-039 (File #005710)
Date notice received by OIPC	May 26, 2017
Date Organization last provided information	December 14, 2017
Date of decision	March 2, 2018
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 under Alberta's *Societies Act* and is a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. Under sections 56(2) and (3), PIPA only applies to personal information that is collected, used or disclosed by non-profit organizations in connection with a commercial activity. "Commercial activity" is defined in section 56(1)(a) of PIPA to mean "any transaction, act, or conduct or …regular course of conduct, that is of a commercial character…". In this case, the Organization provides courses, materials and services for which it charges fees. The information at issue was collected during the course of these activities. In my view, the Organization collected the personal information in connection with a commercial activity and is subject to PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • customer name, • business or employer contact address, • credit card type (no number, CCVV or expiry date), • course information (services and materials ordered, course location, attended/completed, certificate issued), • employer name, • customer role or title,

	• membership status (Y/N), • gender (optional – rarely entered), • date of birth (optional – rarely entered), and • telephone number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses a service provider, Pixel Army, to provide e-commerce services enabling the Organization's members/customers to order courses, materials and services using an internet website. • On May 9, 2017, the Organization learned that an unknown third party, without authorization, accessed the server-end of the Organization's e-commerce website. The Organization reported "It appears that the incident involved an unauthorized ability to access AHSA's website's underlying data for a period of time…". • The Organization reported that "no payment information (no card or account details) was exposed" and further, "limited personal information was potentially exposed, and … there is no evidence that any information was exfiltrated from the site."
Affected individuals	The incident affected 13,714 Alberta residents.
Steps taken to reduce risk of harm to individuals	The Organization reported that its service provider: • Immediately hired a cyber security firm to analyze and identify the compromise. • Built a new server. • Downloaded, manually scrubbed, virus scanned all websites on the server and uploaded the new server. • Scanned all sites on the new server for code vulnerabilities. • Took old server offline. • Recommended short term security fixes which were all implemented. • Completed or implementing long term suggestions.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on October 20, 2017.

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 "there is no risk of credit card fraud, but there may be a small increased risk of identity theft, given the scope of the information exposed." I agree with the Organization. Financial information, such as credit card number, was not compromised in this incident, making it difficult to use information for credit card fraud. However, identity information (such as date of birth) may have been compromised and, in conjunction with other information elements at issue (employment information, gender, telephone number), could be used to cause the harms of 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 "there is little or no potential harm to any public institution, body or organization; there is little potential harm to the payment system as a whole; nor any realistic potential to cause a loss of trust of any particular organization in a larger societal sense; nor any real potential risk of physical harm, security, reputational or relationship harm to the Organization's member/customers whose information was potentially exposed during the relevant period." Further, the Organization's service provider reportedly told the Organization that "The evidence we have supports the server being compromised and that your information was at risk, but nothing to support that it was actually downloaded, etc.". In my view, 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). The Organization did not report how long the information was exposed for. The Organization did not provide information to demonstrate that it had taken steps to confirm information was not downloaded.
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. Financial information, such as credit card number, was not compromised in this incident, making it difficult to use information for credit card fraud. However, identity information (such as date of birth) may have been compromised and, in conjunction with other information elements at issue (employment information, gender, telephone number), could be used to cause the harms of identity theft and fraud. These are 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 (deliberate intrusion). The Organization did not report how long the information was exposed for. The Organization did not provide information to demonstrate that it had taken steps to confirm information was not downloaded.	

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email on October 20, 2017, in accordance with section 19.1 of the PIPA Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner