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	American Health Information Management Association (Organization)
Decision number (file number)	P2021-ND-227 (File #019175)
Date notice received by OIPC	January 25, 2021
Date Organization last provided information	September 21, 2021
Date of decision	November 12, 2021
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 is a non-profit entity located in Chicago, IL, USA, and is an "organization" as defined in Section 1(1)(i) of PIPA. The Organization's report of the incident said although it… *… does not pursue commercial activities, does not provide services in Alberta or Canada, and as such does not consider itself to be subject to the Personal Information Protection Act, [The Organization] is nonetheless providing this report as a courtesy because [it] has experienced a data security incident that may have affected the personal information of Alberta residents obtaining services in the United States and thereby may give rise to a real risk of significant harm for those residents.* Pursuant to section 56(2), PIPA "does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization", except in the case of personal information that is collected, used or disclosed in connection with any commercial activity.

	Section 56(1) of PIAP defines "Non-profit organization" to mean an organization "that is incorporated under Alberta's *Societies Act* or *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act*". In this case, the Organization is located in Chicago, IL and not incorporated as defined above. Therefore, the Organization does not qualify as a "non-profit organization" as defined in section 56(1)(b) of PIPA, despite operating on a not for profit basis, and is not excluded from PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue may have included: • name, • payment card number, expiry date, and security code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information at issue was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization maintains an online store (https://my.ahima.org/store/), through which customers can make purchases and register for courses. • The Organization learned of potential suspicious activity occurring in the online store, took immediate steps to secure its system and conducted an internal investigation. • On December 3, 2020, the Organization's investigation determined that the incident involved the payment card information of customers who made purchases through the online store between June 26, 2020 and June 29, 2020 as well as between October 1, 2020 and October 16, 2020.
Affected individuals	The incident affected 17 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Engaged legal counsel to guide an external investigation and evaluate related notification obligations. • Engaged a digital forensics firm to determine what happened as well as whether the payment card information of customers had been affected. • Reported the incident to the FBI. • Offered affected individuals complimentary credit monitoring and identity protection services for 24 months.

Steps taken to notify individuals of the incident	Affected individuals were notified by email on January 22, 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 did not specifically identify any harm that might result from this incident, but has offered affected individuals complimentary credit monitoring and identity protection services. In my view, a reasonable person would consider that the contact and financial information at issue 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's report of the incident said that it "…has experienced a data security incident that may have affected the personal information of Alberta residents obtaining services in the United States and thereby may give rise to a real risk of significant harm for those residents." In my view, a reasonable person would consider 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 two (2) weeks.
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 contact and financial information at issue 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). Further, the information may have been exposed for approximately two (2) weeks. I require the Organization to notify the affected individuals whose information was collected 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 January 22, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner