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 Association of Nurse Anesthetists (Organization)
Decision number (file number)	P2020-ND-138 (File #014152)
Date notice received by OIPC	December 11, 2019
Date Organization last provided information	December 11, 2019
Date of decision	November 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 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 Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • billing address, • credit card type, number, verification value or expiry date. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's ecommerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization was notified of a potential data incident due to an unauthorized individual gaining access to its ecommerce website and inserting a malicious script designed to capture payment card information entered into the checkout page.

	• The malicious script may have affected information entered on the website between May 23, 2019 and October 3, 2019. • The breach was discovered by the Organization's website host on October 3, 2019.
Affected individuals	The incident affected 787 individuals, including 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Removed the malicious code. • Engaged an outside forensic investigation firm to assist with investigating and remediating the potential incident. • The website host is continuing to enhance security controls and monitor its systems to detect and prevent unauthorized access.
Steps taken to notify individuals of the incident	The Organization reported affected individuals would be notified by letter on December 12, 2019.
REAL RISK OF SIGNIFICANT HAR,M 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 its website host "… has no information that any individual has suffered any harm as a result of the potential incident. Potential harms may include fraudulent transactions." I agree with the Organization's assessment. The contact and financial information at issue could be used to cause the significant harms of identity theft and fraud.
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 its website host "...has no evidence that the code actually captured any personal information. The information involved in this potential incident includes credit card numbers. The Commissioner has held credit card numbers to be highly sensitive. Out of an abundance of caution, [the website host] is notifying potentially affected individuals about this incident [and] is providing information to help these individuals protect themselves." In my view, a reasonable person would consider that the risk of significant harm is increased as the breach resulted from malicious intent (deliberate intrusion), and the information may have been exposed over 4 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 to the affected individuals.	

A reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. The risk of significant harm is increased as the breach resulted from malicious intent (deliberate intrusion), and the information may have been exposed over 4 months.

The Organization is required to notify the affected individual whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

The Organization reported affected individuals would be notified by letter on December 12, 2019. I require the Organization to confirm in writing, within 10 days of the date of this decision, that the affected individual whose personal information was collected in Alberta, was notified.

Jill Clayton
Information and Privacy Commissioner