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 Public Works Association (Organization)
Decision number (file number)	P2021-ND-024 (File #016495)
Date notice received by OIPC	July 21, 2020
Date Organization last provided information	July 21, 2020
Date of decision	February 23, 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 headquartered in Kansas City, Missouri, USA, and 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, • address, • payment card/account number (security codes and expiry date.) This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• The Organization maintains an online store (www.apwa.net/store/), through which members can pay dues, purchase merchandise and educational resources, and register for events.

	• On or about May 8, 2020, the Organization was notified about a potential scripting issue within the software that supports its cloud-based association management software. • On or about May 15, 2020, the Organization was notified that the issue was a vulnerability that presented a security risk because it could facilitate a "man in the middle attack" whereby a threat actor could compromise payment card information at the point of sale in its online store. • On June 23, 2020, the forensics investigation determined that the payment card information of customers who made purchases through the Organization's online store between April 10, 2020 and May 20, 2020 was accessed by an unknown and unauthorized third party, leading to the potential compromise of certain customers' payment card information.
Affected individuals	The incident affected 567 individuals, including 25 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Took affected webserver offline and restored the environment with a new server. • Patched the vulnerability and enhanced the security of its system environment. • Explored additional layers of security. • Notified the relevant payment card brands and working with them to ensure affected individuals' payment card information is protected. • Notified the Federal Bureau of Investigation, as well as payment processing partners, PayPal and Commerce Bank, Visa, MasterCard, and American Express. • Offered individuals one-year of free credit and identity theft monitoring, identity theft insurance and identity restoration services.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on July 17, 2020.
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 affected payment card information may have included names, addresses, card numbers, expiration dates, and security codes." In my view, a reasonable person would consider that the contact and financial information at issue (payment card number, security code and expiry date) 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 assessed the likelihood of harm resulting from this incident as "Low – See details re "risk mitigation" below*".* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's systems is used for fraudulent purposes. Lastly, the personal information may have been exposed for approximately six 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 (payment card number, security code and expiry date) could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's systems is used for fraudulent purposes. Lastly, the personal information may have been exposed for approximately six weeks.

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 in an email July 17, 2002 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner