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	Alpha Industries, Inc. (Organization)
Decision number (file number)	P2018-ND-122 (File #006771)
Date notice received by OIPC	October 5, 2017
Date Organization last provided information	November 15, 2017
Date of decision	September 17, 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 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 all or some of the following information: • name, • address, • email address, • debit or credit card number, expiry date, and CVV verification code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information was collected in Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 25, 2017, the Organization learned that its third-party digital commerce platform provider, Aptos Inc., had experienced an intrusion.

	• The intruder(s) accessed the digital commerce platform and may have acquired certain personal information of customers who manually entered their payment card details on the Organization's website between July 6, 2017 and August 9, 2017. • On September 8, 2017 and again on October 17, 2017, the service provider gave the Organization information regarding potentially affected customers.
Affected individuals	The incident affected approximately 1,500 individuals, including 8 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Engaged a cybersecurity firm. • Removed the malicious code and disabled the page used to gain access to the systems. • Filtered the code to remove non-alphanumeric characters and created an alert that is designed to highlight attempts to modify the code. • Contacted and offered assistance to United States law enforcement. • Offered one year complimentary credit monitoring and an identity theft restoration product. • Established a call centre to provide information to affected customers.
Steps taken to notify individuals of the incident	Two affected individuals were notified by letter on October 23, 2017 and the Organization said an additional six affected individuals were to be notified the week of November 6, 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 "The potential harm, if any, that could arise from this breach is unknown, but might include fraud or negative effects on a credit record". In my view, the financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss. The contact information at issue, as well as email address, could be used for unsolicited emails and phishing. I have previously found phishing to be 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 "The likelihood of harm resulting from the breach is unknown". 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 unauthorized intrusion). Further, the information may have been exposed for approximately one month.

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 financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss. The contact information at issue, as well as email address, could be used for unsolicited emails and phishing. I have previously found phishing to be a significant harm. 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 unauthorized intrusion). Further, the information may have been exposed for approximately one month.

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).

The Organization reported that two of the affected individuals were notified by letter on October 23, 2017 and an additional six affected individuals were to be notified the week of November 6, 2017.

The Organization is required to confirm to my Office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner