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	AmeriCommerce by Cart.com (Organization)
Decision number (file number)	P2021-ND-322 (File #020734)
Date notice received by OIPC	April 23, 2021
Date Organization last provided information	April 23, 2021
Date of decision	March 9, 2022
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 an e-commerce technology company that helps merchants process payment card transactions. The Organization head office is in Texas, USA. 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, • shipping and billing address, • email address, • telephone number, • payment card number, • expiration date, and • CVV. 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	• On March 29, 2021, the Organization identified a security incident involving unauthorized use of the file upload feature of its application to add code to the checkout page of some of its merchant customers. • The code was added to the sites involved at different times starting on March 25, 2021. The Organization removed the code from all sites on March 29, 2021. • Transactions using a stored payment card and transactions entered directly by the merchant were not involved.
Affected individuals	The incident affected 3,581 individuals, including 1 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Implemented additional security measures to harden security on the platform hosting online stores. • Put processes and procedures in place to prevent similar situations from happening and will continue to harden security regularly. • Notified law enforcement. • Notified payment cards network so that they can inform the banks that issued the cards. • Advised individuals to closely review payment card account statements and immediately report any unauthorized charges to the bank that issued the card. • Provided a telephone number for individuals to call with any questions they may have.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on April 23, 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 reported "The consequence of the breach are most likely limited to unauthroized (sic) charges on the involved payment card. Individuals have been notified and encourange (sic) to review their payment card statements and report unauthorized charges. Payment card network rules generally state that cardholders are not responsible for fraudulent charges that are timely reported. [The Organization] has also notified the card brands of which cards were involved." In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to 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, *The likelihood of harm is very low. Payment card network rules generally state that cardholders are not responsible for fraudulent charges that are timely reported.* 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). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 significant harms of identity theft and fraud and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to 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 can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 letter on April 23, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner