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	Springfield, Inc. (d/b/a Springfield Armory) (Organization)
Decision number (file number)	P2016-ND-70 (File #004396)
Date notice received by OIPC	November 21, 2016
Date Organization last provided information	November 21, 2016
Date of decision	December 23, 2016
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 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • email address, • telephone number, • order ID, • payment card number, expiry date, security code (CVV). 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 e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization engaged a cyber security firm to examine its website after receiving a report from a payment card network of unauthorized charges on payment cards used to make purchases on the website.

	• On October 5, 2016, the investigation determined that an unauthorized person(s) gained access to the web server and installed code that was designed to copy information entered during the checkout process. • The incident occurred between October 3, 2015 and October 9, 2016.
Affected individuals	Affected individuals include 11 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Deleted database table containing order information from its web server. • Deleted malicious code and reimaged the webserver. • Strengthened website security through a variety of measures. • Encouraging customers to review payment card account statements and to report any unauthorized charges • Providing a dedicated call center to address any questions affected individuals may have regarding the incident.
Steps taken to notify individuals of the incident	The Organization reported it would be providing written notification to customers who placed orders on the website from October 3, 2015 to October 9, 2016, including 11 residents of Alberta.
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.	In assessing the harm that might result from this incident, the Organization reported that "The order information affected here includes payment card information which is generally used to make fraudulent purchases elsewhere online. However, generally card network regulations provide that cardholders are not responsible for fraudulent charges that are timely reported to the issuer of the card." I agree that the personal information involved could be used to make fraudulent charges, as well as generally cause the harms of identity theft and fraud. These are significant harms that could result to the affected individual as a result of this incident. In addition, email addresses could be used to cause the significant harm of phishing.

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 "Card networks generally have operating regulations that provide that cardholders are not responsible for fraudulent charges that are [sic] timely reported to the bank that issued the card." In my view, the likelihood of harm resulting from this incident is increased because the breach resulted from malicious intent (deliberate intrusion), and the information was exposed for a considerable length of time (approximately 1 year). The Organization can only speculate that the potential harm from this incident will be mitigated by "operating regulations that provide that cardholders are not responsible for fraudulent charges." Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, or phishing.

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.

I agree that the personal information involved could be used to make fraudulent charges, as well as generally cause the harms of identity theft and fraud. These are significant harms that could result to the affected individual as a result of this incident. In addition, email addresses could be used to cause the significant harm of phishing.

The likelihood of harm resulting from this incident is increased because the breach resulted from malicious intent (deliberate intrusion), and the information was exposed for a considerable length of time (approximately 1 year). The Organization can only speculate that the potential harm from this incident will be mitigated by "operating regulations that provide that cardholders are not responsible for fraudulent charges." Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, or phishing.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and provide me with written confirmation that it has done so on or before January 20, 2017.

Jill Clayton
Information and Privacy Commissioner