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	Combat Brands LLC (Organization)
Decision number (file number)	P2018-ND-010 (File #007340)
Date notice received by OIPC	December 12, 2017
Date Organization last provided information	December 12, 2017
Date of decision	January 8, 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 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, • credit and debit card number, • expiry date, and • 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 from residents of Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On April 14, 2017, the Organization reported an incident involving unauthorized access to information systems to the Office of the Information and Privacy Commissioner. Breach notification decision P2017-ND-65 was issued on May 25, 2017.

	• At the time, the Organization believed all malware operating on its websites had been identified and removed. • On October 16, 2017, while running routine scans, the Organization again identified unusual code running on its websites. The Organization retained a new third-party forensic investigator to determine what happened. The new investigators confirmed that the malware was not a new attack but already existed at the time of the original investigation and had not been removed as originally thought. • The previously unidentified malware was removed on October 6, 2017 and investigators have confirmed no other malware exists. • The new investigation confirmed that the malware may have stolen the information at issue from some payment cards used at www.fightgear.com, www.fitness1st.com, www.ringside.com, and www.combatsports.com between July 1, 2015 and October 6, 2017.
Affected individuals	The incident potentially affected 28 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged third-party forensic investigators to determine what happened, what information was affected and to implement additional procedures to further protect the security of customer debit and credit cards. • Removed the malware at issue on October 6, 2017. • Established a dedicated hotline for individuals to contact with questions or concerns regarding the incident. • Providing potentially impacted individuals with information on how to protect against identity theft and fraud. • Providing written notice of the incident to other state regulators and national consumer reporting agencies as necessary.
Steps taken to notify individuals of the incident	The Organization reported it was providing written notice of the incident to potentially impacted Albertans beginning on or about November 29, 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 did not specifically identify any harm that might result from this incident, but reported that it provided potentially affected individuals with information on how to "protect against identity theft and fraud". In my view, the 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 did not specifically assess the likelihood of harm resulting from this incident. In my view, the likelihood of harm resulting from this incident is increased because the incident is the result of malicious action by an unknown third party (deliberate intrusion and malware). The information may have been exposed for over two years.
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 could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the incident is the result of malicious action by an unknown third party (deliberate intrusion and malware). The information may have been exposed for over two years. I require the Organization to notify the affected individuals 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 Alberta beginning on or about November 29, 2017. The Organization is not required to notify the affected individuals again.	

Jill Clayton
Information and Privacy Commissioner