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	I Love Kickboxing LLC (Organization)
Decision number (file number)	P2017-ND-63 (File #005478)
Date notice received by OIPC	April 24, 2017
Date Organization last provided information	April 24, 2017
Date of decision	May 23, 2017
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 all or some of the following information: • first and last name, • street address, • email address, and • credit/debit card information. 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 or about March 24, 2017, the Organization's third-party cybersecurity team determined that the Organization was the target of a sophisticated cyber-attack.

	• The Organization investigated and determined that the personal information of Alberta residents stored on an electronic database may have been accessed intermittently between October 2016 and early January 2017 by unauthorized persons.
Affected individuals	The incident affected two (2) residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Retained a third-party team of forensic technical experts to assess and remediate any security concerns on its system. • Considering options, including moving onto a managed server system and adding further protections to its security systems.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on April 21, 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 "There is a risk that the information was taken with malicious intent and could be used for fraudulent purposes that could lead to identity theft or fraud." I agree with the Organization's assessment. The financial information at issue could be used to cause the significant harms of identity theft and fraud. 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 "There is a risk that the information was taken with malicious intent and could be used for fraudulent purposes that could lead to identity theft or fraud. However, due to the nature of the incident, it is not possible to know if the information was in fact used fraudulently. As such, [the Organization] has taken steps to inform affected consumers of measures that can be taken to prevent identity theft." 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). Despite the fact the Organization reported "it is not possible to know if the information was in fact used fraudulently" and steps taken to inform affected individuals of how to protect themselves, the information was exposed for approximately 3 months, has not been recovered, and may be used in the future for fraudulent purposes.

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. 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 incident is the result of malicious action by an unknown third party (deliberate intrusion). Despite the fact the Organization reported "it is not possible to know if the information was in fact used fraudulently" and steps taken to inform affected individuals of how to protect themselves, the information was exposed for approximately 3 months, has not been recovered, and may be used in the future for fraudulent purposes. 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 in writing on April 21, 2017.The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner