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	YogaFit Training Systems Worldwide, Inc. (Organization)
Decision number (file number)	P2021-ND-025 (File #016512)
Date notice received by OIPC	July 23, 2020
Date Organization last provided information	July 23, 2020
Date of decision	February 23, 2021
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 located in Las Vegas Nevada, USA, and 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, • address, • credit card number (security codes and expiry date), and • username and password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about May 27, 2020, the Organization began investigating a report from a customer of an unusual payment card charge.

	• The investigation determined that the Organization was the victim of a sophisticated cyberattack that may have resulted in a compromise to some of its customers' credit and debit cards used to make purchases on its website, www.yogafit.com, between April 11, 2020 and May 27, 2020.
Affected individuals	The incident affected 735 individuals, including 16 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Took steps to secure its website and launched an in-depth investigation, with the assistance of its web developer, to determine the nature and scope of the incident. • Reviewing existing policies and procedures and implementing additional safeguards to further secure payment information. • Notifying relevant regulatory authorities, as required by applicable law. • Providing potentially affected individuals with guidance on how to better protect against identity theft and fraud.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 22, 2020.
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 that "Possible harms may include identity theft and financial fraud." In my view, a reasonable person would consider that the contact and financial information at issue (payment card number, security code and expiry date) could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. These are all 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.	In assessing the likelihood of harm resulting from this incident, the Organization reported "A limited number of individuals reported suspicious payment card activity." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed for approximately six weeks. Some individuals reported suspicious payment card activity.

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. In my view, a reasonable person would consider that the reasonable person would consider that the contact and financial information at issue (payment card number, security code and expiry date) could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. These are all significant harms. The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed for approximately six weeks. Some individuals reported suspicious payment card activity. I require the Organization to notify the affected individuals whose personal information was collected 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 an email July 22, 2002 in accordance with the *Regulation*. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner