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	RevUp Group, LLC d/b/a RevUp Sports (Organization)
Decision number (file number)	P2019-ND-085 (File #009094)
Date notice received by OIPC	June 29, 2018
Date Organization last provided information	June 19, 2018
Date of decision	June 25, 2019
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • first and last name, • billing and mailing address, • email address, and • credit card name, account number, expiry date, security code. This information is about an identifiable individual 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 May 31, 2018, the Organization became aware that an unauthorized third part(ies) gained access to the Organization's system and installed one or more files that may have collected personal information from customers who made credit card purchases via the Organization's website.

	• The Organization reported that it has not discovered any evidence indicating that the affected information was downloaded or exfiltrated from the Organization's network, but the Organization has been unable to definitively rule out any unauthorized acquisition of data. • The incident occurred from September 19, 2017 to March 20, 2018.
Affected individuals	The incident affected one individual in Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted an investigation. • Performed a security scan and removed all potentially malicious files from its computer system. • Contacted state regulators. • Provided guidance on how affected individuals can better protect against identity theft and fraud. • Offered credit monitoring for affected individuals.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on or about June 21, 2018.
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 "There is a low risk of financial harm." In my view, a reasonable person would consider that the contact and financial information at issue (including credit card number, expiry dates, and security codes) could be used to cause identity theft, fraud and/or 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 that "At this time, [the Organization] does not think the risk of harm is significant [sic]. [The Organization] is not aware of any fraud or identity theft to any individual as a result of this incident and does not know if any information was actually viewed or obtained by an unauthorized party." 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 by an unknown third party. The personal information may have been exposed for approximately 6 months. The lack of reported incidents to date is not a mitigating factor, as phishing, identity theft, fraud and/or financial loss can occur months and even years after a data breach.

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 individual. A reasonable person would consider that the contact and financial information at issue (including credit card number, expiry dates, and security codes) could be used to cause identity theft, fraud and/or 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 as the breach appears to be the result of a deliberate, unauthorized intrusion by an unknown third party. The personal information may have been exposed for approximately 6 months. The lack of reported incidents to date is not a mitigating factor, as phishing, identity theft, fraud and/or financial loss can occur months and even years after a data breach. I require the Organization to notify the affected individual 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 individual in a letter on or about June 21, 2018 in accordance with the *Regulation*. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner