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	National Intramural and Recreational Sports Association (Organization)
Decision number (file number)	P2021-ND-180 (File #017926)
Date notice received by OIPC	November 2, 2020
Date Organization last provided information	May 21, 2021
Date of decision	September 2, 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 those 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 headquartered in Oregon, 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 all or some of the following information: • name, • username, • password, • email address, • mailing address, • telephone number, • employment information, • payment card information, • ethnicity, and • gender. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses a third-party service provider for e-commerce. On or around May 7, 2020, the Organization's third-party vendor reported a known vulnerability impacting the Organization's systems. • The Organization investigated the vulnerability, and on May 26, 2020, became aware of suspicious activity on its e-commerce site. It was discovered that an unauthorized party exploited the vulnerability on April 6, 2020, exposing personal information. The Organization reported ending the breach on June 3, 2020. • On July 13, 2020, the Organization's investigation determined that personal information was exposed in the incident. • Personal information was exposed for approximately 58 days.
Affected individuals	The incident affected 272 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Retained a computer forensics firm to determine scope of the incident. • Rebuilt impacted web server. • Improved security protocols. • Notified payment card brands and card processor. • Notified various US state regulators.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 27, 2020, and October 23, 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: *For the majority of the individuals, possible harms are loss of control over personal data and phishing attempts. For the two individuals whose payment card information was exposed, other possible harms could be identity theft or other forms of fraud.* I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the harms of identity theft, fraud, or financial loss. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. Further, credentials could be used to compromise other online accounts. 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: *As outlined above, for the majority of the individuals, the exposed data is limited to name, contact details, ethnicity, member status and employment information. [The Organization] considers that there is not a likely risk of harm to these individuals.* *For the two individuals whose payment card information was exposed, the risk of harm appears unlikely as there is no forensic evidence that this information was accessed and/or exfiltrated. Additionally, [the Organization] has taken many steps to mitigate the risk of harm. It has notified these two individuals and provided them with guidance on how to protect themselves against identity theft or fraud. [The Organization] has also notified the major payment card brands and its card processor of the incident and the steps taken to return to processing payment card transactions securely. [The Organization] is not aware of any misuse of their personal information.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised by an unauthorized party who exploited a vulnerability (deliberate intrusion). The lack of reported misuse of the personal information to date does not mitigate against future harms as identity theft and fraud can occur months or years after a breach. Further, the information may have been exposed for approximately two months (58 days).

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.

A reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the harms of identity theft, fraud, or financial loss. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. Further, credentials could be used to compromise other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised by an unauthorized party who exploited a vulnerability (deliberate intrusion). The lack of reported misuse of the personal information to date does not mitigate against future harms as identity theft and fraud can occur months or years after a breach. Further, the information may have been exposed for approximately two months (58 days).

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 affected individuals by letters dated July 27, 2020 and October 23, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner