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	ACTIVE Network (Organization)
Decision number (file number)	P2018-ND-057 (File #008051)
Date notice received by OIPC	March 19, 2018
Date Organization last provided information	November 5, 2018
Date of decision	May 6, 2019
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 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, • address, • email address, and • credit or debit card number, expiry date and verification code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization provides a platform to host online registration and payment services for athletic races and similar events. • In October 2017, the Organization became aware of suspicious activity on one of its systems through social media activity, customer complaints and reports from the card brands.

	• The Organization investigated and determined the suspicious activity related to transactions manually keyed in by users while checking out on the Organization's website, and that an unauthorized third party may have accessed personal information provided by users between December 2016 and September 2017. • The investigation also determined that the unauthorized third party used customer credentials (i.e. belonging to a race or event organizer) to access the network. The Organization believes the credentials were taken from the customers by way of a phishing attack or social engineering. Because the unauthorized third party used customer credentials, this access did not appear to be unauthorized. The unauthorized third party was able to gain further access into the Organization's environment and the presentation layer of an application that is part of the checkout process.
Affected individuals	The incident affected 576 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged cybersecurity firms to investigate the suspicious activity as soon as it was identified. • Took steps to enhance its monitoring tools and security controls. • Worked with customers to assist them in understanding the incident and the notification process.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 19, 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 it "…considers that the risk of harm to individuals in this case is relatively low in light of the protections provided by consumer credit and debit card providers but may include phishing or attempted misuse of credit or debit card numbers." In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, resulting in increased vulnerability to 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 reported that it "…does not consider that the incident gives rise to …" a real risk of significant harm. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately ten months. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, resulting in increased vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately ten months. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 letter on March 19, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner