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	Arabian Horse Association (Organization)
Decision number (file number)	P2022-ND-003 (File #022377)
Date notice received by OIPC	July 19, 2021
Date Organization last provided information	July 19, 2021
Date of decision	February 23, 2022
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, • social insurance number or social security number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 20, 2021, the Organization discovered that it was a victim of a cybersecurity incident. An unauthorized third party may have accessed the Organization's accounting server. • The Organization began measures to restore its operations. However, on March 31, 2021, the Organization experienced a second cybersecurity incident.

	• On April 23, 2021, the Organization determined that an unauthorized third party accessed personal information of certain members and prizewinners on February 20, 2021 and/or March 31, 2021.
Affected individuals	The incident affected 7,235 individuals, including 10 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Notified affected individuals. • Offered two years of credit monitoring services. • Adopted password management and endpoint protection software. • Reset passwords to employee accounts. • Restricted network access.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on June 10, 2021.
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, *Some of the information may be usable to conduct identity theft, to conduct fraudulent banking activities, and for future phishing attempts.* In my view, a reasonable person would consider the contact and identity information potentially at risk could be used to cause the significant harms of identity theft and fraud. The Organization also stated that the addresses could be used for the purpose of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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.	The Organization reported that the likelihood that the significant harm will result is *"Low to moderate."* In my view, the likelihood of harm is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Although the Organization reported, "*We have no indication so far that the data is being misused,"* it did not provide any evidence, such as audit logs, to support this conclusion. I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after an incident.

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 the contact and identity information potentially at risk could be used to cause the significant harms of identity theft and fraud. The Organization also stated that the addresses could be used for the purpose of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms. The likelihood of harm is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Although the Organization reported "*We have no indication so far that the data is being misused,"* it did not provide any evidence, such as audit logs, to support this conclusion. I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after an incident. 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 affected individuals by letter on June 10, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Information and Privacy Commissioner