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	Alberta Beef Producers (Organization)
Decision number (file number)	P2021-ND-313 (File #021911)
Date notice received by OIPC	July 4, 2021
Date Organization last provided information	July 4, 2021
Date of decision	March 4, 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 operates on a not for profit basis. Section 56(1) of PIPA defines "non-profit organization" to mean an organization "that is incorporated under the Societies Act or the Agricultural Societies Act or that is registered under Part 9 of the Companies Act." Pursuant to section 56(2), PIPA "does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization", except in the case of personal information that is collected, used or disclosed in connection with any commercial activity. In this case, the Organization is incorporated under the *Marketing of Agricultural Products Act*. Section 17(2) of that Act provides that a commission established under section 17(1)(b) is a corporation. The Organization was established as a commission in 1969. The relevant section of the Alberta Beef Producers Plan Regulation (AR 268/2009 consolidated up to 169/2020) is "The Alberta Beef Producers Plan and Alberta Beef Producers continued under the Alberta Regulation Producers Plan Regulation (AR 336/2003) are continued under this Plan Regulation. All commissions under the Act are not-for-profit corporations."

	As the Organization is established under the *Marketing of Agricultural Products Act*, it is not a "non-profit organization" as defined in section 56(1)(b) of PIPA, despite operating on a not for profit basis. Therefore, PIPA applies because 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, • company name, • email address, and • banking information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. The Organization reported that the personal information at issue is from "vendors", and includes business names and email addresses. "Business contact information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As such, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• The Organization was the subject of a cyber security breach, which began on June 27, 2021 and ended on June 28, 2021.

	• The attacker targeted the Organization's online payment system and gained unauthorized access using stolen credentials of an employee of the Organization. • The attacker was unsuccessful in attempts to make fraudulent payments; however, personal information for some of the Organization's vendors could have been exposed. • The Organization reported, "the attackers plan was to alter the banking details of our vendors to re-direct payments to accounts that the attacker controlled."
Affected individuals	The incident affected 46 individuals whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Considering a new online system. • Upgrading the password policy for the entire office.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on July 4, 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: *Concerned that the private information exposed in the… breach could be used or incorporated in a scam targeting our customers, i.e. phone scam or Phishing e-mail containing their PII.* I agree with the Organization's assessment. A reasonable person would consider that email addresses, particularly in conjunction with financial information, could be used for the purposes of phishing, increasing 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, *The information exposed does not (in itself) create an imminent threat (i.e. bank accounts cannot be accessed with the exposed information); however there's a moderate risk that the private information could be used in a targeted scam against the vendors (i.e. phone scam or phishing email.* 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 (intrusion, unauthorized access).

	Further, it appears personal information may have been exposed for approximately two (2) 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 email addresses, particularly in conjunction with financial information, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

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 (intrusion, unauthorized access). Further, it appears personal information may have been exposed for approximately two (2) 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 email on July 4, 2021 in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner