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	Gay Lea Foods Co-Operative Limited (Organization)
Decision number (file number)	P2021-ND-317 (File #021338)
Date notice received by OIPC	May 27, 2021
Date Organization last provided information	May 27, 2021
Date of decision	March 7, 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 in Alberta 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, • telephone number, • address, • social insurance number, and • banking information (two individuals). 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.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On December 27, 2020, the Organization's core IT infrastructure ("systems") were encrypted with ransomware. • The Organization received a ransom note that indicated the data, including personal information, had been accessed and

	extracted by the threat actor and that, absent payment, sensitive data would be released. • The Organization investigated and determined the cause of the incident was a phishing attack. An employee opened a phishing email, which contained a malicious document. • The Organization reported, "there is no information indicating that any personal information that was taken has been published or distributed by the threat actor".
Affected individuals	The incident affected approximately 2,100 individuals.
Steps taken to reduce risk of harm to individuals	• Worked with an IT security and forensic specialist to investigate, restore systems, and conduct a review. • Provided affected individuals with credit monitoring and identity theft services for 1 year. • Will take implement further actions informed by the results of the forensic investigation, including improved firewall configurations.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and letter on May 28, 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 the possible harms that may occur as a result of the breach were "MIdentity (sic) theft, phishing scams, financial theft, fraud." I accept the Organization's assessment. A reasonable person would consider the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss.
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 threat actor provided … proof of deletion of the data, including personal information" but that the Organization "…determined to notify all affected employees on the basis that PII was accessed / exfiltrated by the threat actor". In my view, a reasonable person would consider 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, ransom demand). The Organization reported personal information at issue was accessed and exfiltrated.

	Although the threat actor provided proof of deletion of the data, the Organization cannot rule out the possibility that a copy of the information remains with the threat actor.

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, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. 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, ransom demand). The Organization reported personal information at issue was accessed and exfiltrated.

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 and letter on May 28, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner