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	E & J Gallo Winery (Organization)
Decision number (file number)	P2021-ND-251 (File #020928)
Date notice received by OIPC	February 19, 2021
Date Organization last provided information	February 19, 2021
Date of decision	December 9, 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 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 about current and former employees, and applicants for employment: • name, • social security number, • driver's license number, • passport number, • payment card number, and/or • financial account number. 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 November 17, 2020, the Organization experienced a cyber incident designed to encrypt files and disrupt its business operations. • An investigation determined that an unauthorized party gained access to the Organization's systems between November 7, 2020 and November 17, 2020, during which time certain information on some servers may have been accessed or acquired. • The Organization reported the breach was discovered on January 15, 2021, when unusual activity occurred on the network.
Affected individuals	The incident affected 19,970 individuals, including 46 individuals whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged cybersecurity firms to investigate and assist with containment. • Enhanced security protocols. • Offered complimentary credit/identity monitoring to affected individuals. • Notified law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on February 19, 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 that it… *…considers that the goal of the threat actor was to encrypt and steal data in an attempt to extract a ransom payment …and not to perpetrate any fraud against individual employees or consultants. Therefore, the consequences of the breach are most likely to be limited to loss of control of personal data. However, it is also possible that the personal data will be disseminated beyond the threat actor or published online.* In my view, 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	The Organization reported, *While [the Organization's] business and information [sic] to use for leverage to obtain ransom was the likely target of the incident, there is some risk that the individual information involved will be disseminated or missused [sic]. [The*

between the incident and the possible harm.	*Organization] has not received any reports that the information has been missused [sic].* 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, ransom demand). The lack of evidence that the personal information has been misused is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, the information may have been available to the unauthorized third party for approximately 10 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 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 lack of evidence that the personal information has been misused is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, the information may have been available to the unauthorized third party for approximately 10 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 letter on February 19, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner