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	Willow Park Wine & Spirits Ltd. (Organization)
Decision number (file number)	P2022-ND-033 (File #023726)
Date notice received by OIPC	October 21, 2021
Date Organization last provided information	October 21, 2021
Date of decision	May 13, 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:
	
	For 25 individuals:
	• electronic funds transfer (EFT) information, including:
	  ○ name,
	  ○ payment amount,
	  ○ institution number,
	  ○ transit number, and
	  ○ account number.
	
	For 3 individuals:
	• driver's licence, or
	• passport information.
	
	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 28, 2021, the Organization was victim to ransomware. The incident was discovered the following morning when employees were unable to access files. • An investigation determined that a "remote worker's laptop was compromised resulting in a compromised connection to the worker's onsite computer and the organization's network. The intruder was able to use access to that computer system to access a shared drive and to deploy the ransomware." • It is not known how the attacker initially compromised the remote worker's account or their laptop. • The Organization confirmed that data was exfiltrated.
Affected individuals	The incident affected 28 individuals.
Steps taken to reduce risk of harm to individuals	• Offered credit and identity theft protection to affected individuals. • Notified law enforcement. • Installed additional IT security products. • Working with an advisor to harden IT environment.
Steps taken to notify individuals of the incident	Some affected individuals were notified by phone on September 29 and 30, 2021. Written notification was sent by mail or email on October 21 and 22, 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 harm to the three individuals whose government identifiers were accessed includes use of the information to assist a malicious actor in attempting identity theft or other fraud and possibly phishing activities. The harm to individuals whose EFT information was accessed is speculative because no contact information was included; however, it is theoretically possible that the information could be used for phishing, including attempts to have banking information changed.* I accept the Organization's assessment. A reasonable person would consider that identity (driver's licence, passport) and financial information at issue could be used to cause the harms of identity theft, fraud, financial loss, and possibly phishing. 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 intruder was malicious. Accordingly, there is more than a bare possibility of harm. Although the risk of harm in this case does not appear to be likely due to the lack of sophistication of the threat actor and the small amount of data exfiltrated, it nevertheless meets the threshold of a "real risk".* I accept the Organization's assessment. 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 a threat actor (deliberate intrusion, deployment of ransomware). Despite the "lack of sophistication of the threat actor", personal information was nonetheless exfiltrated.

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 identity (driver's licence, passport) and financial information at issue could be used to cause the harms of identity theft, fraud, financial loss, and possibly phishing. 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 a threat actor (deliberate intrusion, deployment of ransomware). Despite the "lack of sophistication of the threat actor", personal information was nonetheless 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 phone, and email or mail, between September 29 and October 22, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance