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	Forty Creek Distillery Ltd. o/a/ Campari Canada (Organization)
Decision number (file number)	P2021-ND-239 (File #018773)
Date notice received by OIPC	December 17, 2020
Date Organization last provided information	March 25, 2021
Date of decision	November 30, 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 headquartered in Grimsby, Ontario and is the Canadian affiliate of Campari Group. 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 information in the Organization's "global directory", including: • name, • work email address, • job title, • line manager, • mobile phone number (only as registered in such directory for business purposes), and • "employee identification code" (an internal number used to identify the employee/consultant within the Organization's IT environment). 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 information in the Directory ordinarily qualifies as "business contact information" within the meaning of sections 1(1)(a) and 4(3)(d) of the Personal Information Protection Act. The Company appreciates, however, that unauthorized access to such business contact information by a malicious actor may qualify as a separate disclosure that is not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose", thereby potentially requiring notification. I agree that some of the information may qualify as "business contact information", which 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." Similarly, I agree with the Organization 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" such that it would be excluded from PIPA. As a result, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On November 1, 2020, the Organization detected that it was the target of a malware attack. • The unauthorized actor gained access to certain of the Organization's servers, which included some employee and contractor information contained in the Organization's global email and telephone directory. • The Organization reported it believes the unauthorized actors accessed the network between October 28 and October 29, and perhaps even as early as October 21, 2020.
Affected individuals	The incident affected 148 individuals, including 15 individuals whose information was collected in Alberta.

Steps taken to reduce risk of harm to individuals	• Worked with cyber security experts to limit the unauthorized actor's access and secure the servers. • Cut-off the unauthorized actor's access. • Implemented technological safeguards designed to prevent a similar intrusion from occurring in the future. • Notified the Office of the Privacy Commissioner of Canada. • Reminded employees to practice good password hygiene and to regularly change both their work and personal account credentials. • Encouraged employees to monitor their email accounts and devices for suspicious communications and in particular, any email communication from an unknown external sender which includes links or attachments. • Offered current employees and contractors two years of free credit and identity protection services, and will be extending the same offer to former employees and contractors.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on November 23, 2020 and January 26, 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, *At this time, the Company's IT team and external consultants have only been able to verify the unauthorized actor's access to the Directory, which consists generally of business contact information for current or former employees or independent contractors...it is possible that the information gleaned could be used for the purposes of phishing and so increase the affected individuals' vulnerability to identify theft and fraud.* I agree with the Organization's assessment. A reasonable person would consider that contact information such as name and email addresses particularly in conjunction with other business contact and employment 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… *...given that the subject information had been accessed via deliberate intrusion by an unauthorized actor...there is a limited but real risk of significant harm to the affected individuals arising from the Incident.*

	I agree with 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 (deliberate intrusion) of an unknown third party. Further, it appears the information at issue may have been exposed for approximately two (2) weeks.

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 contact information such as name and email addresses particularly in conjunction with other business contact and employment 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 (deliberate intrusion) of an unknown third party. Further, it appears the information at issue may have been exposed for approximately two (2) weeks.

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 November 23, 2020 and January 26, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner