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	Carnival Cruise Line a division of Carnival Corporation (the Organization)
Decision number (file number)	P2020-ND-105 (File #015225)
Date notice received by OIPC	February 28, 2020
Date Organization last provided information	July 13, 2020
Date of decision	September 23, 2020
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 Organization reported "The affected databases contained application materials and personal data, such as names, contact information, photos, resumes, passport information and other identification documents submitted when applying for employment … or completing the onboarding process". 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	• The Organization engaged a vendor for certain web development, support and related services including the design and configuration of a job portal hosted on Amazon Web Services cloud computing infrastructure (AWS).

	• On October 29, 2019, the vendor advised the Organization that an intruder had deleted two databases from the portal. The vendor determined that a legacy module not used but available in the codebase was the cause of the incident. • The Organization does not have evidence of unauthorized access or use of the information in the databases. However, this cannot be ruled out. Further, the attacker demanded a ransom.
Affected individuals	The Organization reported that the incident affected approximately 22,000 individuals, including 4 Alberta residents (the Organization acknowledged this number could change).
Steps taken to reduce risk of harm to individuals	• Blocked outside access and applied several hotfixes on the code to eliminate and prevent further exploits. • Changed environment credentials and relevant SSL certificates, and recreated the databases with different configurations. • Commenced an internal security audit to ensure unwanted access or further exploits do not occur. • Seeking to identify and implement additional security measures and monitoring tools.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident by email on February 26, 2020.
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 "…does not have evidence indicating identity theft or misuse of personal information occurred as a result of this incident. However, the OIPC has previously found that similar types of information, if accessed and exfiltrated, could be used for fraud and potentially identity theft". In my view, a reasonable person would consider the contact, employment and identity information at issue could be used to cause the significant harms of 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 OIPC previously concluded that unauthorized access to similar types of information could result in a real risk of significant harm: P2017-ND-131 (McDonald's Restaurants of Canada Limited)." 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 malicious action (deliberate action, ransom demand). The Organization said it has

	no evidence that the information was misused or used for identity theft purposes but "cannot rule this out".

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, employment and identity information at issue could be used to cause the significant harms of 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 malicious action (deliberate action, ransom demand). The Organization said it has no evidence that the information was misused or used for identity theft purposes but "cannot rule this out".

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 the affected individuals by email on February 26, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner