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 Corporation & plc and its subsidiaries and brands (Organization)
Decision number (file number)	P2020-ND-076 (File #015447)
Date notice received by OIPC	March 9, 2020
Date Organization last provided information	March 9, 2020
Date of decision	July 24, 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 the 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's head office is in Miami, Florida, USA. 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 employees, crew members and guests: • name, • address, • Social Insurance Number, • government identification numbers (e.g. passport numbers or driver's license number), • credit card and financial account information, and • health-related information. 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	• In late May 2019, the Organization identified suspicious activity on its network and initiated an investigation. • The Organization discovered that between April 11 and July 23, 2019, an unauthorized third party gained access to some employee email accounts that contained personal information regarding employees, crew, and guests. • Approximately 124 employee email accounts, primarily at Princess Cruise Line, were compromised. • The Organization reported that it appears that the unauthorized third party sought information related to payments and invoices. • On September 19, 2019, the investigation further revealed on that personal information of customers was affected. • The Organization reported that it does not have evidence indicating identity theft or misuse of personal information because of this incident.
Affected individuals	The incident affected 372,000 globally of which 2,487 were individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified law enforcement. • Offered free credit monitoring and identity theft protection services. • Forced a password reset for all email accounts suspected to have been accessed by unauthorized actor(s). • Enabled multi-factor authentication.
Steps taken to notify individuals of the incident	The affected individuals were notified by press release and by letter, beginning March 2, 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 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 that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. These are all 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: P2019-ND-12 (Luxury Hotels International of Canada, ULC a wholly-owned subsidiary of Marriott international, Inc.).* 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 into employee email accounts). The Organization said it has no evidence that the information was misused; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for approximately three months.

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 the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms.

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 into employee email accounts). The Organization said it has no evidence that the information was misused; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for approximately three months.

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 news release and letter beginning on March 2, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner