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	Expedia (Organization)
Decision number (file number)	P2021-ND-115 (File #008856)
Date notice received by OIPC	June 1, 2018
Date Organization last provided information	June 1, 2018
Date of decision	April 20, 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: • full name, • payment card information, • date of birth, • telephone number, • email address, • physical and/or billing address, and • gender. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization acquired Orbitz in 2015. Orbitz operates a travel booking platform. • The Organization reported that "While conducting an investigation of the platform, Orbitz determined on March 1, 2018 and informed us on April 12, 2018, that there was evidence suggesting that, between October 1, 2017 and December 22, 2017, an attacker may have accessed certain personal information stored on its consumer and business partner platform".
Affected individuals	The incident affected five (5) individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Took immediate steps to investigate the incident and enhance security and monitoring of the affected platform. • Acted to eliminate and prevent unauthorized access to the platform.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 10, 2018.
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 potential harm(s) that might result from the incident are "Financial loss, fraud, identity theft, and negative effects on a credit record". 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. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. 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 did not provide its assessment of the likelihood of harm resulting from this incident but did report "To date, Orbitz does not have direct evidence that this personal information was actually taken from the platform." In my view, a reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information appears to have been compromised as a result of malicious intent (unauthorized access by an "attacker"), and the information was exposed for almost 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. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of significant harm resulting from this incident is increased because the personal information appears to have been compromised as a result of malicious intent (unauthorized access by an "attacker"), and the information was exposed for almost 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 affected individuals were notified by letter on May 10, 2018, in compliance with the Regulation. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner