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	SBE ENT Holdings, LLC (Organization)
Decision number (file number)	P2018-ND-101 (File #006123)
Date notice received by OIPC	July 25, 2017
Date Organization last provided information	February 21, 2018
Date of decision	September 17, 2018
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 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • payment card number, expiry date, and possibly security code. In some cases, the following information is also at issue: • name, • email address, • telephone number, • address, and • other information associated with a reservation. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was processed through an online central reservations system. To the extent that the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On or about June 6, 2017, the Organization was notified by its service provider, Sabre Hospitality Solutions (Sabre), that an unauthorized party gained access to certain Sabre account credentials. This permitted unauthorized access to unencrypted payment card information and select reservation information for certain reservations processed and stored on Sabre's central reservations system (CRS). • Sabre facilitates the booking of hotel reservations by guests, including for some hotels that are owned, licensed, or managed by the Organization. Sabre advised the Organization that some of the persons impacted by the unauthorized CRS access were persons who made reservations at the Organization's hotels. • The period of unauthorized access was from August 10, 2016 to March 9, 2017.
Affected individuals	The incident affected 40 individuals whose records indicated they were located in Alberta. However, provision of location information to the Organization is not mandatory. Therefore, there may be other residents of Alberta whose information could have been impacted.
Steps taken to reduce risk of harm to individuals	The Organization reported that its service provider: • Engaged a cybersecurity firm to investigate, and notified law enforcement and payment card brands about the incident. • Has taken measures to help ensure that the unauthorized access to the impacted systems was stopped, and has enhanced security to help prevent further unauthorized access to reservation records processed on its systems.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter starting on July 31, 2017 and a second mailing was done on September 8, 2017. For those affected individuals for whom the Organization was unable to determine a location, the Organization issued a press release on July 21, 2017 respecting the incident, and also notified media.
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 the incident could result in "Potential for fraudulent credit card charges". In my view, the contact, financial and profile information at issue could be used to cause the harms of identity theft, financial loss, and fraud. In addition, email address could be used to cause the harm of phishing. 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 that it "There is a real risk that the harm described above could occur as the information was accessed by an unknown party and the unauthorized access was not detected by Sabre for approximately six months". The Organization also reported its "understanding that the payment card issuers were notified of the unauthorized access … and therefore, [the Organization] expects that the issuers will be monitoring for potential fraud. In addition, generally card network regulations provide that cardholders are not responsible for fraudulent charges that are timely reported to the issuer". In my view, the likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion) and the personal information was exposed for almost seven (7) months. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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.

The contact, financial and profile information at issue could be used to cause the harms of identity theft, financial loss, and fraud. In addition, email address could be used to cause the harm of phishing. These are all significant harms. The likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion) and the personal information was exposed for almost seven (7) months. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

I require the Organization to notify the affected individuals in Alberta accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by letter commencing on July 31, 2017 in accordance with the Regulation. The Organization also issued a press release regarding the incident on July 21, 2017, and notified media. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner