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	Preferred Hotel Group (Organization)
Decision number (file number)	P2018-ND-065 (File #006631)
Date notice received by OIPC	September 25, 2017
Date Organization last provided information	September 25, 2017
Date of decision	May 14, 2019
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: • name, • email address, • telephone number, • address, • reservation information, and • payment card number, expiry date and potentially security code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some information was collected in Alberta via an online central reservation system.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On June 6, 2017, the Organization was notified by its third party reservation service provider, Sabre Hospitality Solutions, that an unauthorized party gained access to the SynXis Central Reservations system. • The service provider's investigation found that the unauthorized party first obtained access to unencrypted payment card and other reservation information on August 10, 2016. The last access was on March 9, 2017.
Affected individuals	The incident affected 466 Alberta residents.
Steps taken to reduce risk of harm to individuals	Reported the breach to law enforcement, payment card brands and the major U.S. credit reporting agencies.
Steps taken to notify individuals of the incident	The Organization notified affected Alberta residents either by mail or email, based on available contact information.
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 "Unauthorized access to payment card information can increase the risk of payment card fraud…". I agree with the Organization's assessment. A reasonable person would consider that the financial information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and harm.
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 as assessment of the likelihood of harm resulting from this incident but reported that "…cardholders are generally not responsible for fraudulent charges" and "At this time, we are unaware of any fraudulent activity that has occurred as a result of the breach". In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion). Further, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing or identity theft and fraud can occur months and years after a data breach. The Organization can only speculate that affected individuals may 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. A reasonable person would consider that the financial information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and harm. The likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion). Further, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing or identity theft and fraud can occur months and years after a data breach. The Organization can only speculate that affected individuals may 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 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 mail or email. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner