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	Luxury Hotels International of Canada, ULC (the Organization), a wholly owned subsidiary of Marriott International, Inc. (Marriott), the primary operating company for Canadian hotels. Marriott acquired Starwood Hotels & Resorts Worldwide, Inc. (Starwood) in September 2016. Starwood brands include: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels. Starwood branded timeshare properties are also included.
Decision number (file number)	P2019-ND-127 (File #010354)
Date notice received by OIPC	November 30, 2018
Date Organization last provided information	July 9, 2019
Date of decision	August 7, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
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 initially reported that it believes the database involved in the incident… *…contains information on up to approximately 500 million guests who made a reservation at a Starwood property…on or before September 10, 2018. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes*

	payment card numbers and payment card expiration dates, but the numbers were encrypted … There are two components needed to decrypt the numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the vast majority of the information was limited to name only, and sometimes other data such as mailing address, email address, or other limited information. In January 2019, the Organization reported "Marriott now believes that approximately 8.6 million encrypted payment cards were involved in the Incident. Of that number, approximately 354,000 payment cards were unexpired as of September 2018." And further, "Marriott now believes that approximately 5.25 million unencrypted passport numbers were included in the information accessed by an unauthorized third party. The information accessed also includes approximately 20.3 million encrypted passport numbers. There is no evidence that the unauthorized third party accessed the master encryption key needed to decrypt passport numbers." 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	• On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. • In its report of the incident, the Organization said "Marriott recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database." • In its original report of the breach, the Organization said that "Marriott has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property… on or before September 10, 2018." • The Organization also reported that "Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014."

Affected individuals	In May 2019, the Organization updated its report of the breach with respect to the "total number of guest records that were involved in the incident", saying: *… After additional analysis, Marriott now believes that that estimated count is approximately 339 million guest records…Marriott had previously estimated that there were approximately 14 million guest records with a country/region address associated with Canada, as determined through the prior deduplication process. Following additional analysis, Marriott now believes that the estimated count is approximately 12.8 million guest records.* The Organization also reported: a. *Marriott's analysis counted approximately 1.8 million involved guest records for which the province address was Alberta, as determined in the deduplication process.* b. *Approximately 55,900 unique encrypted payment card numbers were contained in guest records for which Alberta was the only province ["Marriott believes that the data involved in the incident could also include several thousand unencrypted payment card numbers."]* c. *Approximately 9,870 unencrypted passport numbers were contained in guest records for which Alberta was the only province.* d. *Approximately 12,300 encrypted passport numbers were contained in guest records for which Alberta was the only province.*
Steps taken to reduce risk of harm to individuals	• Installed an endpoint security tool on devices across the Starwood network during the investigation. • Blocked malicious files and tools installed during the incident. • Enhanced security, including logging and monitoring, further segmentation, and multi-factor authentication, as well as password resets and vulnerability scanning. • Phasing out Starwood systems and accelerating ongoing security enhancements to the network. • Reported the incident to law enforcement and payment card brands.
Steps taken to notify individuals of the incident	The Organization's initial report of November 30, 2018 said: *Today, Marriott will begin sending emails to affected guests if an email address is available in the Starwood guest reservation database. Marriott has also released a statement to media outlets, and posted information about*

	the incident and answers to frequently asked questions at www.info.starwoodhotels.com. Marriott has also established a dedicated call center to answer questions that individuals may have about the incident. The call center is open seven days a week and available in multiple languages with phone numbers appropriate for different geographic locations...". The Organization later reported… *… on January 4, 2019, certain information on the dedicated website established for the Incident at https://info.starwoodhotels.com will be updated, and Marriott intends to issue a Form 8-K furnished to the U.S. Securities and Exchange Commission. The 8-K, updated website information, and a press release will include certain of the results of Marriott's further data analysis on the number and types of guest records identified as having been involved in the Incident, as summarized below.* Further, "Marriott has a claims process in place for guests whose passport numbers have been verified to be part of this unencrypted group through the lookup process described above and who are concerned that their information was used fraudulently."
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 did not specifically identify the possible harm(s) that could be cause to affected individuals as a result of the breach. In my view, a reasonable person would consider the identity (date of birth, passport number) and financial (payment card information) at issue could be used to cause the significant harms of identity theft and fraud. Email addresses, particularly in combination with other personal information elements, could be used for phishing purposes, increasing vulnerability to identity theft and fraud.
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 specifically assess the likelihood of harm resulting from this incident. However, in its January 2019 update, the Organization said "There is no evidence that the unauthorized third party accessed either of the components needed to decrypt the encrypted payment card numbers." Further, "While the payment card field in the data involved was encrypted, Marriott is undertaking additional analysis to see if payment card data was inadvertently entered into other fields and was therefore not encrypted. Marriott believes that there may be a small number (fewer than 2,000) of 15-digit and 16-digit numbers in other fields in the data involved that might be unencrypted payment card numbers."

	In my view, a reasonable person would consider the likelihood of harm resulting in this case is increased because the incident appears to be the result of deliberate, malicious action ("an unauthorized party had copied and encrypted information, and took steps towards removing it") and the information may have been exposed for 4 years ("since 2014") before Marriott received an alert. To the extent the only affected information for an individual was encrypted, the risk of harm will be significantly reduced. However, this will only be the case where the Organization can confirm the information was encrypted and not accessible to unauthorized individuals, and no other personal information was compromised.

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 identity (date of birth, passport number) and financial (payment card information) at issue could be used to cause the significant harms of identity theft and fraud. Email addresses, particularly in combination with other personal information elements, could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

The likelihood of harm in this case is increased because the incident appears to be the result of deliberate, malicious action ("an unauthorized party had copied and encrypted information, and took steps towards removing it") and the information may have been exposed for 4 years ("since 2014") before Marriott received an alert. To the extent the only affected information for an individual was encrypted, the risk of harm will be significantly reduced. However, this will only be the case where the Organization can confirm the information was encrypted and not accessible to unauthorized individuals, and no other personal information was compromised.

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 that, as of November 30, 2018, the Organization began notifying affected individuals through various means, both directly and indirectly, and I understand this includes those individuals whose personal information was collected in Alberta.

Nonetheless, I require the Organization to:

- **confirm to my office in writing, within 10 days of the date of this decision, that affected individuals whose personal information was collected in Alberta have been notified in accordance with the Regulation, and**
- **provide details of that notification, including a copy of the email message and date(s) sent.**

Jill Clayton
Information and Privacy Commissioner