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, a wholly owned, indirect subsidiary of Marriott International, Inc. (Organization)
Decision number (file number)	P2020-ND-199 (File #015588)
Date notice received by OIPC	March 17, 2020
Date Organization last provided information	June 29, 2020
Date of decision	December 16, 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 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 Marriott is an international hospitality company whose business includes operating, franchising and licensing hotels that are owned by third party property owners. 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: • contact details (e.g., name, mailing address, email address, and telephone number), • loyalty account information (e.g., account number and points balance, but not passwords), • additional personal details (e.g., company, gender, and birthday day and month), • partnerships and affiliations (e.g., timeshare partner ownership affiliations), and • preferences (e.g., stay/room preferences and language preference). 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 February 26, 2020, the Organization discovered a higher than normal amount of lookup activity on its guest reservation application associated with login credentials of two employees of a franchisee property in Russia. • The change in volume associated with one set of credentials started on January 11, 2020, and the other on January 14, 2020. • On June 29, 2020, the Organization reported it had identified a small amount of prior unauthorized lookup activity between September 21 and December 28, 2018, which it believes is likely connected to and part of the unauthorized access described above. The additional activity involved the credentials of two employees at another of the Organization's properties in Moscow, which were used to access the same application. • The Organization found evidence of connections between some of the individuals who it believes may have been involved in the 2018 activity and those previously identified as being involved in the above unauthorized access. • The Organization identified approximately 228,000 additional queries connected to the 2018 activity which it believes were either successful lookups of additional guest records, failed lookups (e.g. a lookup of a number that did not correspond to any guest profile), or duplicate lookups of guest records already identified. • The Organization reported that no further detail is available about these additional queries, including the identity of any guest records.
Affected individuals	When combined, the incidents affected approximately 17,600 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Established a dedicated website and dedicated call centre resources for customers to obtain more information. • Put in place additional monitoring and restrictions for the loyalty accounts of affected guests and evaluating whether additional protective steps might be required. • Disabled the employee login credentials involved and implementing enhanced monitoring protocols to identify any additional high-volume look-ups. • Disabled loyalty members' passwords and prompted to change their passwords.

	• Prompted members to enable multifactor authentication. • Identifying potential additional security enhancements. • Offered personal information monitoring services, free for a year. • Offered further steps customers can take to protect their personal information (e.g. guarding against phishing, attempts to access the member's loyalty points, and not providing payment card information to anyone that contacts them). • Notified individuals whose information may have been accessed. • Notified relevant authorities and supporting their investigations. • Updated website and call centre resources and sent email notifications to guests resident in Alberta whose valid email addresses were included in the information involved in the 2018 unauthorized activity.
Steps taken to notify individuals of the incident	On March 31, 2020, the Organization issued a press statement and made available a dedicated website and call centre resources in response to the incident on March 31, 2020. On June 24, 2020, the Organization sent email notifications to individuals affected by the 2018 incident.
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, "At this time, [the Organization] does not believe that any individual has suffered any harm as a result of this incident…". However, in its notification to affected individuals, the Organization offered personal information monitoring services and provided information on protecting against identity theft, fraud and phishing attempts. In my view, a reasonable person would consider that the contact and comprehensive profile information (including stay history and point balance), particularly in combination with email address, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are 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 originally reported, "At this time, [the Organization] does not believe … that the incident gives rise to a real risk of significant harm to affected individuals." The Organization subsequently reported: *…the lookups involved in the unauthorized access (including the 2018 activity) are likely to have been connected to attempts to identify [Organization] loyalty accounts with enough loyalty points to use to book a stay. [The Organization] has identified*

	1,082 accounts that appear to have been accessed without authorization, of which only two (2) relate to an accountholder believed to be resident in Alberta. Neither of these two accounts appear to have had fraudulent redemption of …loyalty points. All 1,082 accounts have been locked and are subject to heightened monitoring and security procedures… *The general manner of the unauthorized lookups involved in the 2018 activity appears to have been the same as for the lookups identified in the unauthorized access. [The Organization] therefore believes that the containment and systems remediation measures that it has already implemented are appropriate to prevent a recurrence of the activity.* 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 a third party (deliberate, unauthorized access). Although the Organization has enhanced safeguards, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's application were to be used for fraudulent purposes. The lack of reported fraud to date is not a mitigating factor as identity theft, fraud and phishing attempts can happen months and even years after a data breach. Finally, the information may have been exposed for up to 22 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 and comprehensive profile information (including stay history and point balance), particularly in combination with email address, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate, unauthorized access). Although the Organization has enhanced safeguards, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's application were to be used for fraudulent purposes. The lack of reported fraud to date is not a mitigating factor as identity theft, fraud and phishing attempts can happen months and even years after a data breach. Finally, the information may have been exposed for up to 22 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 affected individuals by email on March 31, 2020 and on June 24, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner