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	Radisson Hospitality Inc. (Organization)
Decision number (file number)	P2018-ND-137 (File #010011)
Date notice received by OIPC	October 11, 2018
Date Organization last provided information	October 11, 2018
Date of decision	October 22, 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 whose 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, • address, • email address, • company name in some cases, • physical address, • rewards member number, and • frequent flyer number. 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 in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On September 11, 2018, a malicious user account was created by an attacker who used stolen credentials to access the system administrator functionality in the customer service application on systems operated and maintained by the Organization. • On October 1, 2018, the Organization activated its Incident Response procedures and the malicious use connectivity was promptly revoked. • The malicious activity was detected through automated behavioral analytics on September 25, 2018. Prior to that date, the unauthorized activity was minimal and within normal operating thresholds.
Affected individuals	The incident affected 1,961,257 individuals, of which 10,745 were individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Revoked access to compromised account and removed all ability for the account to be used while preserving previous account actions and logged new failed login attempts. • Conducted an investigation including internal interviews, malware scanning, and network access blocks. • Review of Incident Response. • Analyzed data of suspected account.
Steps taken to notify individuals of the incident	Affected individuals were not notified.
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 it "believes that the impact on the individuals concerned is limited given the nature of the data involved." In my view, a reasonable person would consider the individual's name, email address and profile information could be used for phishing purposes. This is a significant 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 reported that the likelihood that harm will result is "Low". In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and creation of a malicious account). Further, the information may have been exposed for approximately three weeks.

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 individual's name, email address and profile information could be used for phishing purposes. This is a significant harm. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and creation of a malicious account). Further, the information may have been exposed for approximately three weeks. 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). The Organization is required to confirm to my Office, **within ten (10) days** of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner