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	RWH Travel Limited (Organization)
Decision number (file number)	P2019-ND-159 (File #013138)
Date notice received by OIPC	April 26, 2019
Date Organization last provided information	September 16, 2019
Date of decision	October 24, 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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a travel company based in the UK. While the Organization does not generally carry on business in Canada, nor does it specifically target its services to Canadian individuals, it does have a small number of Canadian customers. 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 some or all of the following information: • name, • date of birth, • postal address, • email address, and • passport numbers (issue and expiry dates). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• On February 14, 2019, the Organization identified a security misconfiguration of an online portal used for internal administrative purposes. This resulted in some customer data potentially being accessible through online search engines when using specific search terms. • The Organization estimates that that the earliest date from which some elements of the data was unsecured was February 1, 2016. The data was secured on February 15, 2019. • The Organization reported that log information indicates the data was accessed by users and search engines, but it is unable to determine if the access was malicious or unauthorized. • The Organization's customer and booking system websites were unaffected by this incident.
Affected individuals	The incident affected 3,167 individuals, including 14 residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted internal investigations into the cause of the incident and to identify documents containing personal information • Revisited and hardened website security. • Reviewed the Organization's internal password policy. • Worked with independent forensic experts to investigate the cause and review the Organization's approach in hardening the fire and web server/source code security. • Planning to implement initiatives to improve regulatory compliance. • Reviewing data handling protocols and will conduct a penetration test to validate the security fixes. • Offered complimentary 12-month membership to monitor personal data for signs of identity theft.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 29, 2019.
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 any harm that might result from this incident, but reported that "…all Canadian individuals will be offered a 12 month membership to [a credit monitoring service] free of charge. This will help them to monitor their personal data for certain signs of potential identify theft." In my view, a reasonable person would consider that the contact and identity information could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to identity theft and fraud. 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 did not specifically assess the likelihood of harm resulting from this incident, but reported "…this is not an incident where we were a specific target by threat actors seeking to steal personal data". The Organization also advised affected individuals that "…there is no evidence *of* any inappropriate or malicious use of impacted data". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased as the breach did not result from malicious intent but rather a misconfiguration of an online portal. However, the information was potentially exposed for approximately 3 years. Despite the fact the Organization reported that "there is no evidence of any unauthorized or malicious use of the data", the Organization did report the information was accessed, and it is unable to determine if such accesses were unauthorized or malicious.

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 identity information could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to identity theft and fraud. These are all significant harms. The likelihood of harm resulting from this incident is decreased as the breach did not result from malicious intent but rather a misconfiguration of an online portal. However, the information was potentially exposed for approximately 3 years. Despite the fact the Organization reported that "there is no evidence of any unauthorized or malicious use of the data", the Organization did report the information was accessed, and it is unable to determine if such accesses were unauthorized or malicious.

I require the Organization to notify the affected individuals 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 dated April 29, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner