July 16, 2019

# UK Information Commissioner Confirms Intention to Fine British Airways and Marriott International, Inc Under GDPR

**Attorneys**
Rohan Massey
Clare Sellars

On 8 July 2019, the UK Information Commissioner (**ICO**) issued a statement in response to an announcement to the London Stock Exchange of its intention to issue British Airways (**BA**) with a monetary penalty of £183.39 million for breaches of the General Data Protection Regulation (**GDPR**). The next day the ICO issued a further statement in response to Marriott International, Inc's (**Marriott**) filing with the US Securities and Exchange Commission regarding its intention to issue Marriott with a monetary penalty of £99,200,396 regarding certain (unrelated) GDPR breaches.

The statements note that both BA and Marriott have cooperated with the ICO investigations and improved their security arrangements since the breaches were discovered. Both organisations will be given the chance to make representations regarding the ICO's proposed findings and monetary penalties. Under the GDPR's one-stop-shop mechanism, other EU data protection authorities whose residents have been impacted will also be able to provide comments on the ICO's findings. The ICO will consider all representations before finalizing its decisions.

## The Breaches

The proposed British Airways fine relates to an incident that BA brought to the ICO's attention in September 2018 regarding a cyber-attack (believed to have started in June 2018) involving the personal data of around 500,000 BA customers. User traffic to the BA website was directed to a fraudulent site through which certain customer details were obtained by fraudsters. The affected personal data included names, addresses, log-in details, travel booking details and payment card information. Following its investigation, the ICO has concluded that this incident resulted from inadequate security arrangements by BA.

The proposed penalty represents 1.5% of BA's worldwide turnover for the financial year ended 31 December 2017. The UK Information Commissioner, Elizabeth Denham, commented: "*People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights.*"

BA's chairman and chief executive commented: "*We are surprised and disappointed in this initial finding from the ICO. British Airways responded quickly to a criminal act to steal customers' data. We have found no evidence of fraud/fraudulent activity on accounts linked to the theft. We apologise to our customers for any inconvenience this event caused.*" International Airlines Group's (BA's parent company) chief executive confirmed that BA will defend itself, commenting: "*British Airways will be making representations to the ICO in relation to the proposed fine. We intend to take all appropriate steps to defend the airline's position vigorously, including making any necessary appeals.*"

The proposed Marriott fine also relates to a cyber-attack in respect of the Starwood guest reservation database that Marriott made the ICO aware of on 30 November 2018. Various types of personal data included in around 339 million guest records throughout the world were compromised (around 30 million related to residents of 31 EEA countries, with seven million relating to UK residents).

The ICO has conducted an extensive investigation into the incident, which is thought to have originated in 2014 when the Starwood hotels group's systems and guest reservation database were breached. The breach involved certain guest information regarding reservations on or before 10 September 2018 including names, contact details, passport numbers and, in some cases, payment card information. Marriott acquired Starwood in 2016, but the breach was not exposed until

2018. The ICO's statement notes that Marriott "*failed to undertake sufficient due diligence when it bought Starwood and should have done more to secure its systems.*" The Information Commissioner also commented: "*The GDPR makes it clear that organisations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected.*"

Like BA, Marriott has confirmed that it "*intends to respond and vigorously defend its position.*" Marriott's president and CEO commented: "*We are disappointed with this notice of intent from the ICO, which we will contest. Marriott has been cooperating with the ICO throughout its investigation into the incident, which involved a criminal attack against the Starwood guest reservation database…. We take the privacy and security of guest information very seriously …*".

## Comment

Notwithstanding that both BA and Marriott have stressed that they were the victims of criminal attacks and have cooperated with the respective ICO investigations and strengthened their security arrangements, clearly the ICO is not afraid to use its new enforcement powers in cases where serious breaches of the GDPR have occurred as a result of organisations' failure to meet GDPR standards. It is also clear that the ICO expects organisations to carry out comprehensive data protection-related due diligence when making acquisitions and implement appropriate procedures to ensure personal data is secured. In BA's case, the proposed fine could have been worse as, depending on the nature of the breaches considered by the ICO in calculating the fine, the ICO could have proposed a fine of up to 4% (rather than 1.5%) of BA's global annual turnover (or potentially even up to 4% of AIG's global annual turnover, as BA and AIG are part of the same undertaking).