July 15, 2019

Bite in the Tail for British Airways and No Holiday for Marriott

UK Information Commissioner's Office Imposes Fines on Airline and Hospitality Company for Data Breaches

The UK Information Commissioner's Office (ICO) has proposed fines on British Airways (BA) and Marriott International within a span of two days, with BA suffering a potential penalty of £183 million and Marriott £99.2 million, under the Data Protection Act 2018.

The ICO has stated that "personal data has a real value, so organisations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public."

Turbulence Ahead for British Airways

The ICO fine on British Airways was the result of a data breach last year that led to the theft of BA customers' credit card data. Although BA claims no harm was caused to its customers, the Information Commissioner, Elizabeth Denham, was quick to emphasise that such breaches need to be dealt with seriously. Denham said, "People's personal data is just that — personal," and "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 chairman and chief executive, Alex Cruz, commented: "We are surprised and disappointed in this initial finding from the ICO."

Key Takeaways:

The proposed £183 million and £99.2 million fines against British Airways and Marriott, respectively, by the UK's ICO emphasise:

1. The need for companies to maintain appropriate data protection practices for personal data under their control.
2. An increased focus in M&A transactions on conducting necessary privacy and data protection due diligence on acquisition targets.
3. After completion of M&A transactions, buyers should address any issues discovered during due diligence and conduct additional data protection audits and remediation.

For more information on data protection and privacy laws, please contact your Katten attorney, the firm's **Privacy, Data and Cybersecurity** group or any of the following:

Christopher Hitchins
+44 (0) 20 7776 7663
christopher.hitchins@kattenlaw.co.uk

Sarah Simpson
+44 (0) 20 7770 5238
sarah.simpson@kattenlaw.co.uk

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Matthew R. Baker
+1.415.293.5816
matthew.baker@kattenlaw.com

Megan Hardiman
+1.312.902.5488
megan.hardiman@kattenlaw.com

Hackers stole both personal and financial information from hundreds of thousands of customers who had booked flights with BA during August and September of 2018. This information included payment card details such as card numbers, expiration dates, CVV numbers and customer names. Then in October 2018, BA announced that customers who had booked flights through its Avios rewards programme in April–July of 2018 were also at risk.

The proposed penalty for BA represents 1.5 percent of BA's total worldwide revenue for 2017. Under the General Data Protection Regulation (GDPR), the ICO is entitled to issue a fine for data breaches of up to 4 percent of an organisation's global annual revenue, or €20 million, whichever is higher. Had the ICO sought to impose the maximum fine, BA could have faced a £488 million fine rather than the £183 million currently on the table.

Marriott Merger Headache

One day after announcing BA's fine, the ICO announced its plans to fine the US-based hotel group, Marriott International. The Marriott breach, which was publicised in November 2018, exposed millions of hotel guests' personal data, including credit card information, passport numbers, names, addresses, phone numbers and email addresses. The incident occurred prior to Marriott's 2016 acquisition of Starwood Hotels and Resorts and is believed to date back to 2014, when Starwood's systems were compromised. Since the breach was not discovered until after the acquisition, the ICO found that Marriott's due diligence of Starwood was inadequate, and that the hotel group should have taken greater steps to secure its systems.

The ICO emphasised the significance of due diligence in mergers and acquisitions (M&A) by stating, "The GDPR makes it clear that organisations must be accountable for the personal data they hold." The commissioner continued: "This can include carrying out proper due diligence when making a corporate acquisition . . . [and] . . . proper accountability measures to assess not only what personal data has been acquired, but also how it is protected." Marriott president and CEO, Arne Sorenson, commented: "We are disappointed with this notice of intent from the ICO, which we will contest."

Keep Your Seatbelts Fastened

The size of the fines proposed by the ICO over the last few days — although not the maximum permitted under the law — emphasize the reality of the situation under the new data protection regime. By contrast, under the old data protection laws, telecoms firm TalkTalk was fined a comparatively minimal £400,000 following a cyberattack in 2015, and in 2018, Facebook was fined a relatively minuscule £500,000 for its role in the Cambridge Analytica data scandal.

BA and Marriott have four weeks to appeal, and both have expressed their intent to contest the ICO's fines. BA has stated that it will "take all appropriate steps to defend the airline's position vigorously, including making any necessary appeals." The ICO commented that it "will consider carefully" any representations made by BA before it makes a final decision. However, Cruz's comments regarding the alleged minimal harm done to customers appear unlikely to cut it with the ICO.

BA and Marriott, in addition to the ICO's fines, could also face individual claims from the customers who were affected by the data breaches, not to mention customer and public relations damage given the negative press surrounding the incidents and their handling.

Katten

Katten Muchin Rosenman UK LLP

www.kattenlaw.co.uk

Paternoster House, 65 St Paul's Churchyard • London EC4M 8AB
+44 (0) 20 7776 7620 tel • +44 (0) 20 7776 7621 fax