LATHAM & WATKINS LLP

Global Privacy & Security Compliance Law Blog

Commentary on Global Privacy and Security Issues of Today

UK Regulator Imposes Two Substantial Fines for GDPR Data Breaches

By Latham & Watkins LLP on July 12, 2019

Posted in GDPR

The ICO issued notices of intent to fine British Airways and Marriott. What happened?

By Gail Crawford, Fiona Maclean, Hayley Pizzey, and Calum Docherty

On 8 July 2019, the UK Information Commissioner's Office (ICO) announced a notice of intent to fine British Airways £183.39 million (about US$230 million) for violating the General Data Protection Regulation (GDPR). The proposed fine is the largest to date under the GDPR, and equals 1.5% of British Airways' 2017 global turnover, according to the Financial Times. It follows months of investigation after British Airways notified the ICO of a security incident that led to the theft of customer data in September 2018.

Then on 9 July 2019, the ICO announced a notice of intent to fine Marriott International £99.2 million (about US$124 million) for infringements of the GDPR stemming from a data breach at Starwood, which it acquired in 2016. According to the Wall Street Journal, this fine represents 2.5% of Marriott's global revenue. Marriott initially announced the data breach in November 2018, which led to an ICO probe.

The ICO published its notice of intent to fine in line with its Communication Policy, which provides that whilst the ICO will not routinely publish or publicise preliminary notices or notices of intent "[it] may do so if there is an overriding public interest; all parties agree; the matter is already in the public domain; there are financial market reporting obligations; it is necessary for the purposes of international regulatory cooperation; or if publicising information allows for improved public protection from threat".

The ICO confirmed that whilst they have a number of other investigations and enforcement actions in the pipeline, they may not be disclosed publically at the "intent to fine" stage and companies will have time to make submissions following receipt of the confidential notice to assign. Elizabeth Denham said "we didn't disclose this fine for British Airways nor did we disclose it for Marriott. Those companies had a confidential notice of intent and they had marke

obligations to disclose it. They decided. So we followed up with a statement. That's why you don't see the full report with all the details. Usually this is a confidential exchange".

What were the underlying breaches?

British Airways

British Airways' data breach reportedly involved a cyberattack on the airline's website and app, by which hackers diverted British Airways' customers to a fraudulent website to harvest customer information. The incident affected approximately 500,000 individuals. The categories of personal data compromised reportedly include: customer names, postal addresses, email addresses, log-in data, credit card data (including CVV data), and booking information. The ICO stated that the incident is believed to have begun in June 2018, and that it was notified of the incident in September 2018. (British Airways has stated in public reports that the incident took place from 21 Augus 2018 to 5 September 2018). Statements from the ICO referenced "poor security arrangements" resulting in data being compromised, implying that the investigation included a review of the airline's security measures. Elizabeth Denham, the UK Information Commissioner, stated, "The law is clear — when you are *entrusted with personal data, you must look after it"*.

Marriott

Marriott first discovered information from its guest reservation database had been stolen in September 2018. It had acquired the compromised database as part of its purchase of Starwood properties in 2016. Unauthorized access to the system reportedly dated back to 2014. The breach affected over 300 million customers, including 30 million residents of the European Economic Area. The personal data compromised reportedly included: customer names, postal addresses, phone numbers, dates of birth, gender, email addresses, loyalty program account information, reservation information, five million unencrypted passport numbers, and eight million encrypted credit card numbers. Marriott did not believe the security vulnerability in Starwood's database affected its own reservation system and has since phased the compromised database out of operation. Marriott has cooperated with the ICO investigation and has subsequently improved its security arrangements.

What happens next?

The ICO's notice of intent triggers a process whereby British Airways and Marriott can submit representations in response to their respective penalties. This process lasts a period of not less than 21 days (the ICO will set out the exact period in each notice). The ICO's regulatory enforcement policy states that representations should be submitted in writing, though in exceptional cases, the ICO may grant oral meetings. The representations may cover how the breaches occurred, present mitigating information, what actions the companies have taken, and details on any further remediation steps. Further, the representations may put forth arguments as to why the ICO should not take regulatory action, and request a reduced penalty. Penalties over £1 million may justify convening a panel of non-executive advisors to the ICO to make a recommendation to the Commissioner based on the representations submitted. British Airways' parent company announced it planned to make representations to the ICO and "take all appropriate steps to defend the airline's position vigorously", while Marriott confirmed its intent to "vigorously defend its position".

Under the GDPR's one-stop-shop mechanism, the ICO, acting as the lead supervisory authority, shares its findings with other EU concerned supervisory authorities (*i.e.*, in jurisdictions where other individuals have been affected)

after British Airways and Marriott make their representations; these regulators will then have the opportunity to comment.

Regardless of the ICO's process, British Airways faces additional risk in the form of collective proceedings by affected customers before the English High Court. Consumers in the group litigation are reportedly seeking up to £2,000 each on average, which could cost the airline tens of millions of pounds over the ICO's fine. (So far, public statements reveal that about 5,500 people have agreed to take part in the collective proceedings, which would yield additional costs of £11 million, if successful; the cost could potentially reach £1 billion if all 500,000 affected claimants join.) Marriott is subject to class action consumer litigation for negligence in the US. Initial complaints seek up to US$12.5 billion in damages for 500 million affected customers.

These ICO notices of intention are a clear sign that the UK regulator is not afraid to issue large fines to try and improve behaviour and ensure companies takes data security seriously. The Marriott fine, in particular, highlights the importance of conducting thorough information technology diligence before acquiring a company. The Information Commissioner warned, "[O]rganisations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition."

This post was prepared with the assistance of Sanjana Parikh in the London office of Latham & Watkins.