July 10, 2019

U.K. Regulator Announces Hefty GDPR Fines for Cybersecurity Failures

This week, the U.K. Information Commissioner's Office ("ICO") announced that it intends to fine two public companies hundreds of millions of dollars for alleged violations of the European Union's General Data Protection Regulation ("GDPR"), signaling enhanced GDPR enforcement, both in the cadence of enforcement actions and the magnitude of fines imposed.

The intended £99.20 million fine against Marriott International arose from a security vulnerability discovered in 2018 that exposed the personal information of approximately 339 million guests of the Starwood hotel group, which Marriott acquired in 2016. According to the ICO, Marriott "failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems." In a statement accompanying the announcement, the Information Commissioner emphasized that the GDPR requires that companies carry out "proper due diligence when making a corporate acquisition."

The intended £183.39 million fine against British Airways stems from a 2018 cyber incident where user traffic on the company website was diverted to a fraudulent site, allowing the personal data and payment card information of approximately 500,000 customers to be stolen. Though British Airways was a victim of the attack and reported it to the ICO, the investigation concluded that the data was compromised due to "poor security arrangements at the company," in violation of the GDPR requirement that companies implement appropriate data security measures. The intended fine represents about 1.5% of the company's worldwide annual revenue.

These two fines would be the largest under the GDPR to date, exceeding the €50 million fine against Google earlier this year (discussed here), and dwarfing the biggest pre-GDPR penalty imposed by the ICO of £500,000. Both companies have announced that they intend to contest the ICO's intended penalties.

These enforcement actions underscore the importance of addressing cybersecurity risks as a function of sound corporate governance (as discussed here). The Delaware Supreme Court's decision in *Marchand* v. *Barnhill*, which we recently addressed, is a stark reminder that boards have a fiduciary duty under the *Caremark* line of cases to exercise oversight over key compliance risks. Cybersecurity has proven to be a vital risk—one that increasingly should be

addressed through effective risk management and active oversight at the board level.

As the Marriott action demonstrates, and we have advised previously, companies involved in M&A transactions should engage in careful diligence of data privacy and cybersecurity risks, especially in situations where the GDPR applies. Companies are now on notice that their due diligence may be subject to significant scrutiny in hindsight, whether completed before the GDPR took effect or currently. Due diligence investigations of data privacy and cybersecurity risks should be carefully documented to withstand after-the-fact scrutiny.

European data protection authorities are likely to pursue additional major GDPR enforcement actions. While the magnitude of the fines imposed on Marriott and British Airways are significant, the GDPR provides for maximum fines that could be as high as 4% of a company's annual worldwide revenue. Given the heightened stakes, companies should ensure that they are employing robust data security practices, regular vulnerability assessment and remediation procedures, and careful due diligence of cybersecurity and data privacy risks in connection with M&A transactions, with active oversight by senior management and boards of directors.

David A. Katz
Marshall L. Miller
Daniel H. Rosenblum