Corporate Compliance Insights

ICO to Issue More Than $350M in Fines Under the GDPR

Record Fines for British Airways and Marriot

By Daniel Alvarez and Henrietta de Salis I August 20, 2019 *in* Data Privacy, Featured

In light of news of substantial fines from the U.K.'s ICO, Willkie Farr & Gallagher attorneys discuss the importance of safeguarding and understanding the personal data in a company's possession – whether its own or acquired through corporate transactions.

In two statements released this week, the U.K. Information Commissioner's Office (ICO) announced its intention to fine both British Airways and Marriott International for infringements of the General Data Protection Regulation ("GDPR") in connection with data breaches reported by those companies in 2018. The proposed fines would be the two largest penalties levied against a company under the GDPR by any regulator in the U.K. The ICO's announcement follows the French data protection authority's action earlier this year, in which it fined Google €50 million (approximately US$56 million) for violations of the GDPR related to transparency and consent. The ICO's announcements and accompanying fines highlight the importance of safeguarding and understanding the personal data in a company's possession, whether its own or acquired through corporate transactions.

The ICO will take account of any representations by British Airways and Marriott and other EU member states' data protection authorities before taking its final decision.

British Airways: A Record-Setting Fine

On July 8, 2019, the ICO announced that it intends to fine British Airways £183,390,000 (approximately US$230 million) for violations of the GDPR related to a cybersecurity incident in which malware on the airline's website diverted user traffic to a fraudulent site where attackers were able to harvest customer details. The personal data (including credit card information) of approximately 500,000 customers was compromised in the incident. Following an extensive investigation, the ICO asserted that poor security measures at British Airways enabled the data breach and justified the proposed penalty. While the ICO noted that the airline has made improvements to its security program following the incident, the GDPR requires covered entities to implement appropriate security measures and to notify supervisory authorities and individuals of data breaches if certain thresholds are met. The proposed fine is by far the

highest imposed under the GDPR to date, but it could have been higher. The proposed fine is equal to 1.5 percent of the airline's global turnover for financial year 2017. The GDPR permits penalties up to 4 percent of annual revenues.

British Airways, in a statement to investors by its parent company, IAG, has stated that it found no evidence of fraudulent activity on accounts linked to the incident and that it intends to vigorously defend itself against the proposed fine.

Marriott: Spotlight on Data Security in Due Diligence

The day after its British Airways announcement, the ICO announced its intention to fine Marriott International £99,200,396 (approximately US$124 million) in connection with a breach of its Starwood guest reservation database that affected approximately 339 million guests. Marriott discovered and disclosed the incident in November 2018, though the compromise in Starwood's systems likely took place in 2014 — before Starwood was acquired by Marriott in 2016

In its announcement of the proposed penalty, the ICO highlighted the importance of privacy and data security due diligence in deals to ensure compliance with the GDPR and asserted that Marriott had failed to undertake "sufficient due diligence" and "should have done more to secure its systems" when it acquired Starwood in 2016. The U.K. Information Commissioner Elizabeth Denham noted: "The GDPR makes it clear that organizations 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."

Moving Forward

Unfortunately for most companies, these announcements have raised more questions than they have answered. We will ultimately have to wait and see if the ICO will issue detailed findings and guidance on some of the specific points raised, such as what qualifies as "sufficient due diligence" in corporate acquisitions. An implication of the ICO's statement regarding its investigation of Marriott is that sufficient due diligence would have given Marriott the opportunity to, or require Starwood to, put in place adequate data security measures over customer data. The ICO has noted that Marriott has made improvements to its data security arrangements since the breaches came to light. In the meantime, these announcements reinforce that regulators intend to use their significant authority to impose fines granted by the GDPR, and the Marriott announcement in particular highlights that buyers and sellers alike should thoughtfully consider privacy and data security issues when assessing risk as part of the M&A due diligence process. And while the ICO's announcement specifically highlights this need for any deal that might involve EU personal data subject to the GDPR, it remains the case that even deals outside of the GDPR's scope should include careful review of privacy and data security issues as well, as evidenced by the 2016 Yahoo/Verizon deal, in which Verizon was able to negotiate $350 million off of Yahoo's purchase price due to previously undisclosed security breaches.

Daniel Alvarez and Henrietta de Salis

Daniel K. Alvarez is a partner in Willkie Farr & Gallagher's Communications & Media Department in Washington. He is also a member of the Cybersecurity & Privacy Practice Group. Daniel brings an extensive background in technology and regulatory issues to counseling a broad range of clients in diverse industries on privacy and cybersecurity issues, including financial and health care privacy, regulation of marketing and advertising practices, international data transfer, children's privacy and other privacy and cybersecurity matters regulated by the FTC, FCC, SEC and other state and federal agencies.

Henrietta de Salis is a U.K. partner in Willkie's London office and a member of the Asset Management, Corporate & Financial Services, Structured Finance & Derivatives and Data Privacy & Security practice groups. Henrietta provides advice and transaction support to banks, securities firms, asset and investment managers, funds and intermediaries — including broker-dealers, custodians, trading platforms, private equity firms, wealth managers and insurers — on U.K. and European financial services legislation and compliance matters in both the wholesale and retail markets.

This article and others can be accessed through Willkie Compliance Concourse, a free, on-demand, web-based app providing access to practical guidance and the latest developments in regulatory compliance, investigations and enforcement, available at https://complianceconcourse.willkie.com.

WILLKIE FARR & GALLAGHER LLP