Proposed £99 Million Marriott GDPR Data Breach Fine Underscores Importance of Cybersecurity in M&A

July 16, 2019

Dramatically upping the ante on cybersecurity in the context of mergers and acquisitions, the UK Information Commissioner's Office ("ICO") has announced its intention to fine Marriott £99 million for apparent GDPR violations. The proposed fine relates to a highly publicised data breach at Starwood, a company acquired by Marriott. We offer here a summary of what is publicly known about the ICO action, and some thoughts on how companies might raise their game when it comes to cyber diligence in the M&A sphere.

Debevoise & Plimpton

The proposed Marriott fine is the first major regulatory action anywhere to specifically call out a company for purportedly inadequate cyber due diligence in connection with an M&A deal. The proposed fine comes hot on the heels of the ICO's notice of intent to fine British Airways £183 million. That proposed fine relates to British Airways' 2018 data breach affecting approximately 500,000 customers.

The ICO has not yet published the details of Marriott's alleged GDPR violations. Hence it remains to be seen exactly what more the ICO thinks Marriott could or should have done to identify and remediate the Starwood breach, whether pre- or post-closing of the acquisition.

Based on the ICO's announcement, the breach originated in a system belonging to the Starwood hotels group, which Marriott acquired in 2016. The relevant Starwood systems apparently were compromised in 2014, but the exposure of customer data was only discovered in 2018. By that point, the breach is said to have affected 30 million people within the European Economic Area ("EEA")–touching all 31 EEA member states–including 7 million in the UK. The global estimate is that 339 million individuals were affected.

The ICO's press release states that Marriott failed to undertake sufficient due diligence when it acquired Starwood and that it should have done more to secure its systems. This is an important reminder of the need for all companies–whether subject to GDPR or to other legal regimes–to conduct thorough information security and cyber due diligence pre-acquisition; to obtain appropriate contractual protections in the deal process

through representations, warranties and indemnities; and to give priority to secure integration of systems post-closing an acquisition.

This message is by no means restricted to the EU, and is gaining traction amongst regulators globally. For example, the New York Department of Financial Services' cybersecurity regulation FAQ states that Covered Entities (essentially banks and insurers, wherever headquartered, that carry a licence to operate in New York) must have "*a serious due diligence process and cybersecurity should be a priority when considering any new acquisitions,*" and that Covered Entities should have written policies and procedures covering cybersecurity due diligence.

The challenges of pre-closing cyber diligence are well known. Cyber will always be competing for dealmakers' attention with a host of other issues. There is only so much oxygen in the dealmaking room, and cyber has not often been seen as a major driver of valuation. (This despite headline-making examples, such as Verizon imposing a $350 million haircut on Yahoo! in 2017 when Verizon learned about a major Yahoo! breach between the original agreement over the deal and closing.) Even when the acquirer makes cyber diligence a priority, target companies may be reluctant to disclose their cyber risks at a useful level of detail.

The result of these and other challenges is that robust cyber diligence, as often as not, has only occurred post-closing. The proposed ICO fine to Marriott and the New York DFS guidance suggest that companies on both sides of the deal table may now want to give greater priority to these issues earlier on. Steps to consider include:

- Adding cyber-focused resources to the acquirer's due diligence team, including counsel with cyber expertise and outside experts in cyber forensics.

- Including more, and more detailed, cybersecurity questions on due diligence questionnaires than has historically been typical.

- Making those questions focused and specific–such as requesting access to particular records, such as penetration test results, risk assessments, and internal and external reports of particular cyber incidents and investigations–so that vague or general responses are more difficult for the target to give and the target's cybersecurity program and resiliency to cyber threats can be fully understood and examined.

- Being sure to include in the diligence phase an opportunity for candid, direct discussions between senior cyber-savvy people from both the target and acquirer, such as each side's chief information security officers.

- Drafting cybersecurity reps and warranties that are specific enough to have real bite, and making them enforceable post-closing either explicitly, or indirectly through bespoke rep and warranty insurance policies that specifically address post-closing cyber risk. The only likely limitation from an insurance perspective will be the underwriting appetite for the specific deal. That said, representations that there have been no data breaches pre-acquisition that have had, or will have, a material effect on the target commonly only survive for one to one-and-a-half years post-closing. Given the length of time breaches often remain undiscovered, such representations might provide limited comfort to the buyer in reality. Acquirers may also be faced with the reality that requesting aggressive cybersecurity representations may put them at a disadvantage in a competitive auction process.

- Reviewing the target's cybersecurity insurance to ascertain whether it provides coverage for GDPR penalties and, if so, whether the acquirer will be able to benefit from it or will have to rely on its own cover. Companies should be aware, though, that coverage is commonly limited to the extent a GDPR fine is insurable under the law of the relevant jurisdiction, something that remains unclear in many places and may well be litigated in the future if the ICO and others continue their aggressive enforcement agendas.

Post-closing cyber diligence also might usefully be elevated in terms of priority and resources. Here too, outside expertise can be useful, as can promptly making a specific action plan to assess the risks at the acquired company, then creating targeted risk mitigation plans with clear milestones and appropriate budget authority.

Listed companies should also remain vigilant of the potential need to notify the market when breaches occur and at key points thereafter. Like with British Airways, the ICO made its announcement in response to a regulatory filing: here, Marriott's update to the U.S. Securities and Exchange Commission in which it disclosed a possible fine by the ICO. Listed companies need to consider carefully when to disclose data breaches to the market and when to issue public updates or make regulatory filings on any follow-on litigation or enforcement action and what steps might be needed to prevent insider trading on that information.

With Marriott having publicly stated that it intends to "vigorously defend its position"–in what many will view as a troubling case, given the genuine challenges that any acquirer faces in cyber diligence–it might be some time before the ICO issues its final penalty. Regardless of how long it takes for the ICO and Marriott to resolve this particular matter, the lessons for how to address cybersecurity in the M&A context are vivid and immediate.

With members of its Cybersecurity & Data Privacy Group on both sides of the Atlantic, Debevoise is well-placed to assist EU and non-EU businesses on all areas of GDPR compliance, including cyber incident preparation, incident response, and interaction with data protection authorities.

* * *

Please do not hesitate to contact us with any questions.

LONDON

Jane Shvets
jshvets@debevoise.com

Christopher Garrett
cgarrett@debevoise.com

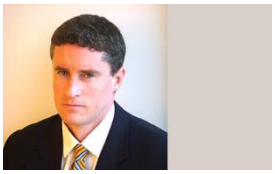
Robert Maddox
rmaddox@debevoise.com

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Paul M. Rodel
pmrodel@debevoise.com



Keith J. Slattery
kjslattery@debevoise.com

Stephanie M. Cipolla
smcipolla@debevoise.com

WASHINGTON, D.C.

Jeffrey P. Cunard
jpcunard@debevoise.com

Luke Dembosky
ldembosky@debevoise.com