PUBLICATION

Privacy & Cybersecurity Due Diligence – No Longer Optional: Company Fined $124 Million for Pre-Merger Compromise

Authors: Alisa L. Chestler, Andrew Jacob Droke
July 29, 2019

In early July, a global hospitality company announced in a U.S. Securities and Exchange Commission (SEC) filing that it had been fined more than $124 million (more than £99 million) by the United Kingdom's Information Commissioner's Office (ICO). The fine, which is equal to 2.5 percent of their worldwide annual revenue, stemmed from the November 2018 announcement of a 2014 breach of a reservation database maintained by a company acquired in 2016. The accounts of up to 383 million guests were potentially compromised as a result of the incident.

While many are focused on the general headline that the fine stemmed from violations of the General Data Protection Regulation (GDPR), the ICO's statements show that it focused on the company's failures to identify the breach both during due diligence conducted prior to the 2016 acquisition and during the two years of operations following closing. In announcing the fine, the Information Commissioner stated:

"The GDPR makes it clear that organisations 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."

All organizations contemplating any M&A activity must pay heed, as diligence regarding a target's information privacy and cybersecurity practices is no longer optional.

In addition to potential post-closing liability, cyber-related diligence can affect the target's valuation and the viability of a proposed transaction. In 2017, Yahoo lost $350 million in value after breaches were disclosed during Verizon's acquisition of the company.

To ensure an accurate understanding of the risks and vulnerabilities, buyers should want to know as much as possible regarding the target's privacy and cybersecurity practices pre-closing, as the consequences can be significant. Conducting robust diligence in this area can also assist with remediation planning and integrating the target's systems post-close.

Baker Donelson's Data Protection, Privacy, and Cybersecurity Team routinely assists organizations with privacy and cybersecurity diligence and with addressing the related risks in the M&A context. For more information, please contact Alisa Chestler or any member of Baker Donelson's Data Protection Team.