Due Diligence of Corporate Data Assets In M&A Transactions: Data Protection/Privacy

03.21.2019

As data are quickly becoming significant corporate assets, lawyers need to help companies both maximize the value of their data and protect the business against any associated risks. This is particularly true in M&A transactions, as acquiring companies often will not have much insight into the data assets held by the target company. Failing to identify and address those risks can result in significant costs to the acquiring company.

There are a number of considerations a potential buyer should consider with respect to data assets. These include privacy/data protection, intellectual property rights in data, issues associated with data quality and liability and regulatory considerations. This post will outline due diligence issues associated with data protection and privacy. In the future, the Williams Mullen Data and Privacy Dispatch will examine the other issues from a due diligence perspective.

Part 1 - Privacy and Data Protection Due Diligence

Due diligence in M&A transactions for privacy and data protection issues has become increasingly important after reports of several high-profile data breaches of target companies that occurred before acquisition. For example, in November 2018 Marriot announced a data security incident involving the Starwood guest reservation database. The unauthorized access, which occurred prior to Marriot?s acquisition of Starwood in 2016, opens Marriott up to significant regulatory penalties and potential civil damages. Similarly, Verizon reportedly reduced its purchase price for Yahoo by $350 million due to two large data breach incidents that occurred prior to the signing of the acquisition documents but before closing.

Data protection/privacy due diligence can be placed into six primary buckets:

Data ? It is critical for the buyer?s counsel to identify what personal data assets the target company has collected and how they were acquired, used and stored in order to ensure compliance with applicable laws and policies. It is often helpful to prepare a data inventory,

including mapping the location as to where data are stored, so as to better identify all potential laws that may apply. A key question is whether offices based in different countries have shared data, as governments increasingly are regulating cross-border data transactions, even within a company.

Data Protection/Privacy Policies ? All companies should have a private statement as to how they use and protect personal information collected from their website. It is critical to ensure that the target company has complied with these statements as a failure to comply is a common way that businesses risk regulatory exposure. Most companies should also have internal data protection policies and procedures. These include privacy policies, information and cybersecurity, training, data breach response plans, and business continuity plans. It is important to review these policies to make sure they are current, are adequate from a legal standpoint and have been followed from an operational standpoint. If not, additional questions should be asked.

Cybersecurity ? It is important to understand what cybersecurity measures the company has implemented. Unfortunately, for many businesses there is no specific legal requirement, other than their contractual obligations, as to what level of cybersecurity is required. Rather, an adequate level of cybersecurity protection is based upon a number of factors, including the size of the business and the amount and type of data assets the company collects and stores. As a result, due diligence should focus on why the company determined that its cybersecurity measures were adequate and why it decided against taking additional measures.

Litigation and Regulatory Matters ? Litigation due diligence should include an understanding as to whether the target company has been sued, or threatened with a law suit, for failing to protect personal information or otherwise violating an individual?s privacy. Other considerations include whether the company has received (or has reason to believe that it will receive) any inquiries or notices from federal or state regulators or attorney generals? offices regarding data security? It would also be helpful to know if the target company ever conducted an analysis as to whether data breach notification was required, even if the conclusion was that it was not.

Third parties ? It is important to understand what agreements the target company has with vendors and customers with respect to personal information. This includes understanding what vendors have access to the company?s personal information and whether the related agreements are adequate regarding data security, indemnification, insurance, etc. It is also important to understand what representations or covenants the target company has made to customers and other third parties with respect to personal information and whether it has complied with these obligations. Such obligations can be found in a wide range of agreements, including cloud storage agreements, licenses, software as a service agreements (SaaS) and service level agreements (SLAs).

Insurance ? The target company?s data protection and cybersecurity insurance coverage should always be reviewed as part of any M&A due diligence. As businesses grow they often do not increase their insurance coverage or limits. Therefore, key considerations include whether the coverage is adequate both in scope and coverage limits. In addition, cyber-related

coverage can vary, so it is important to understand what is covered ? and what is not covered ? and how these coverages fit into your company?s risk profile. Similarly, it will be important to identify if coverage will extend beyond closing as many data breaches may not be discovered for months, or even years.

Related People

- Kevin D. Pomfret ? 703.760.5204 ? kpomfret@williamsmullen.com