HUNTON& WILLIAMS

Client Alert

May 2017

Privacy and Data Security Due Diligence in M&A Transactions

Privacy and data security issues have become the subject of critical focus in corporate mergers, acquisitions, divestitures and related transactions. In 2016 and 2017, several large transactions, especially those involving telecommunications, entertainment and technology companies, have been impacted by either concerns about the collection and use of personal information or significant information security breaches. The Federal Trade Commission has sharpened its focus on the use of personal information as a factor in evaluating the competitive effects of a given corporate transaction, and the Securities and Exchange Commission is now closely scrutinizing privacy and data security representations made to investors in public filings connected to transactions. More broadly, privacy and data security problems that are not timely discovered before entering into an M&A transaction can become significant liabilities post-closing and also lead to litigation.

The Importance of Thorough Due Diligence

Because of this heightened concern, it is imperative that companies conduct thorough due diligence about privacy and data security issues before entering into a transaction. The goals of the due diligence process should be to help the parties in a transaction understand (1) what promises and representations a company has made with respect to privacy and data security; (2) whether a company needs to obtain any consents from consumers, employees or others post-transaction to be able to use the personal information previously collected; (3) how the parties' information security programs are structured; (4) how the company has responded or could potentially respond to significant data breaches; and (5) the buyer's potential liability for privacy and data security issues post-closing.

To accomplish these goals, companies should prepare a comprehensive privacy and data security due diligence checklist that it can use for a variety of transactions. The checklist should (1) ask specific questions about privacy and data security issues, such as the types of personal information collected, the parties that may access such information and how such information is transferred within and outside the organization and (2) request relevant privacy- and security-related materials such as privacy notices, information security policies and procedures, incident response plans, privacy and information security training materials, contracts with third-party service providers and any internal and external privacy compliance reviews, assessments or audits.

The due diligence checklist should be customized based on the profile of the target entity and the industry in which it operates. If personal information is at the heart of a transaction, the checklist will usually be quite granular and may involve the provision of ancillary documents such as data flow maps. In addition, certain types of companies such as health care providers and financial institutions must consider sector-specific rules that may impact the nature and structure of the transaction. Finally, the due diligence should also reflect scope, risk tolerance and timing considerations.

Any limitations on due diligence will need to be addressed, such as via the inclusion of more stringent privacy and data security provisions, in the transaction documents. This may include specified indemnities and an escrow account to address potential post-closing liabilities. Limited due diligence also

raises the importance of disclosure schedules — inadequate or incomplete disclosure schedules make it difficult for companies to evaluate the risks associated with a transaction.

Lessons Learned

Companies that fail to conduct proper due diligence into privacy and data security issues in advance of a transaction may run into significant problems following the transaction. These problems may create financial liabilities or prohibit the buyer from using or disclosing customer personal information. Even more impactful, companies may be saddled with material costs related to privacy and data security, such as costs associated with data breach class action litigation, shareholder derivative litigation or government investigations. These post-closing costs often have the potential to destroy any cost-saving synergies that were the impetus for doing the deal in the first place.

Hunton & Williams Can Help

Hunton & Williams has created a cross-disciplinary legal team dedicated to guiding companies through the minefield of regulatory and cyber-related risks associated with high-stakes corporate mergers and acquisitions. The new team brings together the firm's renowned capabilities in privacy and cybersecurity with its recognized strength in M&A transactions.

Contacts

Lisa J. Sotto
lsotto@hunton.com

Steven M. Haas
shaas@hunton.com

Aaron P. Simpson
asimpson@hunton.com

Allen C. Goolsby
agoolsby@hunton.com

Ryan P. Logan
rlogan@hunton.com

Brittany M. Bacon
bbacon@hunton.com