The Harvard Law School Forum on Corporate Governance and Financial Regulation
SUPPORTED BY: CSC CORPORATION SERVICE COMPANY

Key Privacy Issues in M&A Transactions

Posted by Yaron Nili, Co-editor, HLS Forum on Corporate Governance and Financial Regulation, on Tuesday October 21, 2014

Editor's Note: The following post comes to us from Paul A. Chandler, Counsel at Mayer Brown LLP, and is based on a Mayer Brown Legal Update by Mr. Chandler and Lei Shen.

Many merger and acquisition ("M&A") agreements lack specific representations and warranties regarding privacy issues. Often, this is because deal lawyers do not recognize potential privacy risks where the target company (the "Target") lacks e-commerce websites or retail stores that collect consumer data. Nonetheless, significant privacy issues may exist even if the Target is a traditional "brick and mortar" business. Early attention to privacy issues in M&A transaction planning and due diligence can mitigate risks for both buyers and sellers.

Recent high-profile government enforcement actions highlight the need to analyze potential privacy risks. For example, Facebook's acquisition of WhatsApp in February 2014 resulted in the US Federal Trade Commission ("FTC") sending a warning to both companies that the failure to honor WhatsApp's personal data promises to its customers would constitute a deceptive act under the FTC Act. Likewise, Barnes & Noble's recent acquisition of Borders' customer list garnered intense FTC scrutiny due to past promises by Borders not to share its customers' data without their consent.

This article examines key potential privacy issues that may arise in M&A transactions and describes measures that buyers and sellers should take to evaluate and mitigate the risks.

Buyer Concerns

Buyers should conduct thorough due diligence to determine, among other things, (i) the extent to which the Target collects, stores, uses or processes (collectively, "processes") personal data, whether from customers, employees or others, (ii) the nature of the personal data processed, (iii) the countries where the processing occurs and (iv) the Target's current and prior personal data policies and agreements. Special attention should be paid to personal data from EU member countries and other jurisdictions that have stringent privacy laws. Diligence findings should be reviewed with privacy counsel in the relevant jurisdiction(s) to identify legal implications and

compliance issues and to help the buyer draft appropriate representations and warranties to cover potential privacy risks.

The Target's privacy policies are often an important source of information for buyers. These policies include any internal data policies, such as employee privacy policies, as well as any customer-facing privacy policies, such as those posted on the Target's website. Buyers should be on the lookout for failures of the Target to comply with such policies, as well as for restrictions that could be inconsistent with how the buyer plans to use data acquired from the Target. If the Target has current and prior versions of these policies, the buyer should assess (i) whether applicable restrictions are different under each version, (ii) what particular data was collected under (and thus subject to) each version and (iii) how such data is stored (e.g., separately by policy version or segregated). Policy restrictions that impact the buyer's intended use of data should be evaluated to identify steps needed to comply with such restrictions (e.g., obtain consent from the individuals affected).

If the proposed M&A transaction involves the transfer of personal data across national borders, the buyer should review the Target's compliance with applicable cross-border transfer restrictions, such as those required by the European Union. For example, if the personal data of EU residents is involved and the seller indicates that the Target is EU-US Safe Harbor certified, the buyer should review the currency of the Target's Safe Harbor certification, as well as the Target's related internal assessments and compliance materials.

If the proposed M&A transaction is structured as a merger or stock purchase, the buyer may be assuming the Target's past liabilities, including those for privacy compliance issues. Accordingly, buyers in such deals should conduct a more comprehensive analysis of the Target's past and current compliance with privacy laws, including with respect to actual or suspected breaches of the Target's privacy policies or IT security.

Even if they do not assume the Target's liabilities, buyers should assess whether the Target complied with applicable privacy laws when it collected such data and any associated limitations on the buyer's subsequent use of the personal data.

Regardless of deal structure, buyers should identify what personal data needs to be transferred to consummate the transaction—such as the Target's employee payroll, medical or other data—and whether any consents or other formalities are needed to permit such transfers.

Finally, if the proposed M&A transaction involves the provision of services from the seller, the buyer should consider the extent and nature of any personal data involved (such as data for

payroll or benefits plan administration services) and ensure that there are appropriate contractual privacy protections for the contemplated services arrangement.

Seller Concerns

Sellers also have privacy concerns in M&A transactions, particularly when disclosing personal data during the due diligence process or prior to closing. Sellers should review the Target's privacy policies and applicable privacy laws carefully to determine what personal data—including that of its employees—it can share during the due diligence process, as well as to evaluate the compliance, data use restrictions and other issues described above.

Sellers should take care to limit disclosure of sensitive information and personal data and to avoid disclosing data that could trigger security breach notification obligations (e.g., Social Security numbers, driver's license numbers, credit card numbers or medical data). Sellers should also require that disclosures be subject to appropriate nondisclosure agreements and be conducted via a secure method that allows controlled access (such as an encrypted virtual data room).

If the proposed M&A transaction involves employee personal data, the seller should avoid sharing such data in instances where doing so would violate applicable privacy guidelines or policies or the employees involved have a reasonable expectation of privacy in the data (e.g., job performance reviews). In addition, for employees outside the United States, the seller should evaluate the laws of the applicable countries, which may, in some cases, require employee notice and consent prior to sharing or otherwise limit disclosure.

Conclusion

Current and evolving legal requirements require timely, substantial attention to privacy issues in M&A transactions, even in deals involving traditional "old economy" businesses. Leaving these issues to the end of a deal can cause delays and increase risk. Careful attention to potential risks, including those described in this article, can help both buyers and sellers to mitigate risk in M&A transactions.