Bloomberg Law

Corporate Law & Accountability Report™

Reproduced with permission from Corporate Accountability Report, 43 CARE, 3/7/17. Copyright © 2017 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

MERGERS AND ACQUISITIONS

Top 10 Key Privacy Issues in M&A Due Diligence

BY KAREN BROMBERG AND DUANE CRANSTON

Privacy and network security measures continue to play an increasingly prominent role in decisions about potential strategic investments and acquisitions. Revelations of Yahoo's historic hacks (which affected over one billion accounts the first time, and 500 million accounts the second), and the company's reaction to these security breaches has affected the timing and terms of Verizon's proposed acquisition of that company, including a $350 million reduction in the purchase price.

The drama surrounding the Verizon deal shows that early, substantive diligence should be conducted on privacy and cybersecurity issues as an integral part of the M&A process for any deal. Leaving these issues to the end of a deal or paying insufficient attention to them can substantially increase an acquirer's risk.

The following are the ten most important privacy issues that potential acquirers should consider in any due diligence review of a target's operations, and that potential targets should review to prepare for a possible sale.

Karen Bromberg is the head of the firm's Intellectual Property and Technology and Privacy and Data Security groups. Karen is a Certified Information Privacy Professional (CIPP) with certifications covering both U.S. and European privacy law. She advises clients on a broad range of privacy and data protection matters, including privacy policies and procedures, regulatory investigations, global compliance, cross-border data transfers, cybersecurity and network intrusion issues, and contractual issues involving privacy and security with an emphasis on litigation avoidance.

Duane Cranston serves as outside general counsel for a number of early to mid-stage companies in industries ranging from technology to health care, representing clients in data privacy, intellectual property licensing, commercial transactions, and employment matters. Duane is a Certified Information Privacy Professional (CIPP) for U.S. privacy law.

1. Identifying the Industry-Specific Regulations and Applicable Laws

The starting point in any privacy due diligence review is understanding which U.S. state, federal and non-U.S. laws apply to the target's business. Specific privacy and security requirements apply to certain industries that are regulated by U.S. federal and state agencies, including, without limitation: (i) the Gramm-Leach-Bliley Act (**GLBA**) (for certain financial institutions under the jurisdiction of the Federal Trade Commission (FTC) and other federal and state agencies); (ii) the Health Insurance Portability and Accountability Act (**HIPAA**) (for certain health-care service providers); (iii) the Children's Online Privacy Protection Act (**COPPA**) (for websites and online services directed to children under the age of 13 that collect and/or use personal information from children); (iv) the Telephone Consumer Protection Act (**TCPA**) (for telemarketers); and (v) the Fair Credit Reporting Act (FCRA) (for consumer reporting agencies).

Potential acquirers of companies that engage in direct digital marketing, including by sending emails or text messages directly to customers, should review how the target company administers these campaigns with a

COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 2330-6300

careful eye toward complying with privacy disclosures and opt-out requirements under U.S. state and federal laws. Potentially applicable laws include the **CAN-SPAM** Act, which empowers the FTC to regulate such communications and can require the implementation of an ''opt out'' procedure (such as an ''unsubscribe'' option) that allows recipients to opt out of receiving any further commercial communications from the target company.

2. Privacy Policies; Term and Conditions

A company's privacy policy across all media is another important and potentially problematic area. The issue here is whether the target company has put in place adequate privacy policies and/or terms of use, and whether the target is in full compliance with such published policies (whether posted on the target's website or provided to customers). This is particularly important for companies that require user registration or otherwise request information from users that may include personal information, such as demographic data or information that could be used—either alone or in conjunction with other information—to identify specific individuals. The FTC has made it clear that companies must disclose their policies for the handling of personal data and that a company's failure to comply with its stated privacy policies constitutes deceptive trade practices and violates Section 5 of the FTC Act even when the company that made them is acquired by another. Civil penalties for such breaches are not insignificant and can rise to $16,000 per violation. State attorneys general may also pursue similar violations.

3. Employee Data and Policies

Every company has personal data about employees, often including Social Security numbers, benefits information, salaries, job performance reviews and highly sensitive medical information. The review of a target's employment policies should include both a company's collection and handling of employee data (including, without limitation, administrative and technical access to sensitive employee data) and policies addressing the protection of company information (including customer data). These issues should be addressed in a company's employee handbook, and/or through the use of nondisclosure agreements that all employees must sign.

4. Data Security Procedures

Potential acquirers or investors should conduct a broad review of a target company's network security measures and procedures. This review may be more critical depending on the specific industry, particularly where companies collect and use financial, health, or other sensitive personal information in connection with the services they provide to their customers. A due diligence review should cover not only the measures taken by the target company to prevent breaches, but also a review of the company's incident response plan for containing, evaluating and eliminating any actual breaches that may occur. A cyber risk assessment early in the process can provide a general idea of the cyber maturity of the target. A cyber questionnaire can provide a good perspective on the cybersecurity aspects of the target's operations. The questionnaire should, at a minimum, cover things such as where sensitive data are located, the fundamentals of the target's computer network and liability exposure, the adequacy and enforcement of the target's policies, and procedures regarding data privacy and security including testing and corrective follow-up, the target's reliance on third-party service providers, and the level of security controls in place to monitor those providers' own policies and procedures.

5. Breach Notification Policies and Procedures

A separate but related issue is a review of a company's breach notification procedures to ensure compliance with relevant federal and state requirements. Where a company's services may be offered and provided primarily or substantially online, it is particularly important that these breach notification procedures are sufficient to comply with the highest state standards currently in place. This review should also focus on the company's administrative procedures for complying with the relevant legal requirements, including designating and training the appropriate personnel to review these requirements and working with legal counsel to carry out these procedures if necessary.

6. Identifying Regulatory Inquiries, Claims, Litigation and Breaches

An obvious area of inquiry is whether the target has received any regulatory inquiries, litigation claims, or complaints concerning its data privacy and security practices, and whether the target tracks claims submitted to it by consumers or to the government. The target should also be asked if and how it has dealt with any prior security incidents and security breaches.

7. Social Media

A company's social media presence, including the use of social media accounts by employees of the company in their professional capacities, should be reviewed for purposes of understanding a company's public presence and any customer interactions that may take place through these platforms.

8. Vendor Security Due Diligence

Agreements with vendors who may have access to the target company's networks or may receive or process any confidential or sensitive information or data should be carefully reviewed to ensure that such vendors are required to maintain sufficient security procedures. Depending on the sensitivity of such data, these agreements may include requiring the vendors to respond to security questionnaires and allowing companies to conduct audits of the vendors' security measures. Additionally, the target company should take steps to ensure that each vendor is provided only with that minimum level of network or information access necessary to enable such vendor to provide the services for which it has been engaged.

 COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 2330-6300

9. Additional State-Specific Requirements

Forty-seven states, as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands have laws requiring consumer notification when there is a security breach involving personal, financial, or health information. Notice may also be required to state regulators, consumer reporting agencies and the media. Most states impose some type of civil liability for failing to comply with breach notification statutes. Thus, knowing whether a breach has ever taken place at the target company and whether the target complied with the breach notification laws should be an important focus of diligence. In addition to breach notification procedures, certain states may have privacy and data security regulations that apply to specific types of online interactions or transactions. These include, for example, security standards required under Massachusetts law (201 CMR 17.00) for companies that collect or store personal information of Massachusetts residents. The California Online Privacy Protection Act (**CalOPPA**) is another state law that sets out specific privacy policy disclosure requirements regarding the collection, use and sharing with third parties of personally identifiable information and user behavior on a company's website.

10. Cross-Border Considerations

For companies with cross-border operations, due diligence should extend to reviewing a company's compliance with international laws in any jurisdiction in which it operates. Privacy requirements under the European Union's privacy directive are substantially higher than those currently in place in the U.S. The EU prohibits the transfer of personal data of its EU residents to countries like the U.S. that have been deemed inadequate with respect to its privacy protections absent the satisfaction of certain additional requirements. Attempts by the EU and the U.S. to harmonize these requirements under a treaty framework have been successfully challenged in the past and are likely to face further challenges in the future though, for the time being, the Privacy Shield, model contracts and binding corporate rules currently provide a framework for the transfer of personal information from the EU to the U.S. An acquirer should review these issues with an eye not only toward how a potential target currently conducts its operations, but also on how these operations may be impacted by a potential acquisition (e.g., evaluating the extent to which an acquisition may result in the international transmission of personal information).

Conclusion

By focusing on these privacy and security issues during the due diligence phase, acquiring companies can ensure that either the purchase price reflects the potential risks, or that the purchase agreement addresses anticipated risks and apportions liability accordingly.