

DIGITAL ISSUES IN M&A

BY DANIEL B. GARRIE, YOAV M. GRIVER, ANTHONY I. GIACOBBE JR., AND WILLIAM M. O'CONNOR

One of the persistent puzzles surrounding mergers and acquisitions activity is its propensity for failure. In theory, a merger or acquisition adds value in multiple ways. Yet, between 50% and 80% are failures. One largely unexamined but important determinant of post-integration success is data due diligence. With the now widespread use and storage of electronic data, data due diligence should play a critical role in pre-M&A due diligence.

As part of due diligence, companies would do well to create an e-discovery checklist. This checklist should cover: (1) the state of the target company's electronically-stored information, or ESI; (2) existing and anticipated legal holds; (3) costs of preserving data for existing or anticipated legal holds; and (4) structured and unstructured data.

First, the state of the target company's ESI is critical. The acquiring company is generally accountable for ensuring that data relevant to an ongoing or anticipated dispute is properly preserved. Accordingly, the parties to a deal should examine existing legacy systems and the data stored within them to identify integration, data loss and data recovery issues that may create substantial costs and dangers in future litigation. For example, where the producing party's own information systems or document retention scheme escalate the costs of production, courts will likely order it to bear those costs. In a brand name prescription drug antitrust litigation, the court ordered a defendant to bear the costs of culling through more than 30 million stored e-mails, and otherwise "bear the burden caused by the firm's choice of electronic storage."

Second, acquiring companies inherit the target's responsibility of preserving and placing litigation relevant data and metadata under legal hold. Identifying these litigation or regulatory holds should be done pre-acquisition. The reality of M&A is that the target's IT professionals, who are most familiar with the content, format and location of potentially relevant data, tend to be the first to face elimination or redeployment. Yet, failing to adhere to legal holds can be

extraordinarily costly. In one case involving an investment bank, the company's repeated failure to comply with an e-mail preservation order resulted not only in an adverse evidentiary inference, but a crucial shifting of the burden of proof, and, ultimately, \$850 million in punitive damages.

Third, electronic evidence must be preserved in its original format and from its original source. Thus, the affiliated costs of legal holds may include the costly preservation of non-business essential hardware, access software and data the acquirer would otherwise abandon.

Finally, the e-discovery checklist should consider what structured and unstructured data will, or will not, be migrated and maintained by the acquirer. A corporation that acquires a company but fails to understand the manner in which the target company managed and maintained record information creates additional liabilities for itself. For example, an acquiring company that unintentionally discards contract-related unstructured data, such as e-mail, risks judicial interpretation of a contested contract based upon the unstructured data produced by its adversary.

These four issues should be on every due diligence/e-discovery checklist. Ignorance regarding the state of a target company's ESI and electronic discovery obligations can lead a company to misvalue an acquisition, and invite subsequent judicial or regulatory penalties from unintended spoliation.

Spoliation is the destruction, material alteration or failure to preserve evidence in pending or reasonably foreseeable litigation. Spoliation sanctions for electronic data destruction can be particularly difficult to anticipate. Many data storage systems delete certain information on an ongoing, prescheduled basis, and no bright-line rule separates sanctionable and non-sanctionable behavior. Further, the exact level of bad intention, or "scienter," required for a spoliation finding is unclear. Given the murky boundaries between sanctionable and non-sanctionable spoliation of ESI,

parties to M&A transactions must be particularly careful to exchange data maps, or disclose systems under holds, as part of proper data due diligence.

In a case involving a U.S. manufacturing company, for example, the court held that senior management's failure to develop or implement a formal, company-wide information retention policy was sufficiently negligent to justify forcing the company to pay the about \$200,000 cost of restoring information from backup tapes. And, in a wrongful termination case in the Southern District of New York, a firm's employees deleted e-mails relevant to the case well after the firm was instructed to place a litigation hold on them. As a sanction, the jurors were instructed they could infer the deleted e-mails supported the plaintiff's claim. The jury returned a \$29 million verdict against the firm.

These cases illustrate the importance of proper document management policies, senior management's involvement in crafting such policies, and the importance of following legal holds. These items should be a part of every due diligence checklist.

In addition to a proper checklist, parties contemplating a merger or acquisition would be well advised to consider other data-related issues during the M&A process, including valuing and protecting online property, cybersecurity and online trademark issues.

Web sites can be major sources of revenue -- the domain name *sex.com* is a \$100 million property. An acquirer must make sure domain names are properly registered, and property interests in Web sites clearly assigned through domain name transfer agreements. Online property also carries certain attendant risks that should be explored prior to acquisition.

With the increasing use of sensitive personal data in online transactions, the target or merging company's cybersecurity should be considered in any M&A deal. In one case against a firm that sold personal consumer information, the Federal Trade Commission obtained civil penalties for \$15 million after the firm's systems were successfully hacked. Likewise, in the matter of **Petco Animal Supplies Inc.**, the FTC sued Petco for lapses in its Web site security. Eventually, Petco was forced to undertake a comprehensive cybersecurity

overhaul, and agree to independent audits every two years for 20 years.

Further, virus attacks are now considered foreseeable. In one telecommunications case, a public utilities commission levied a fine of more than \$40,000 against a services company because the firm failed to take reasonable, prudent or timely steps to secure its systems against the "slammer worm" virus.

Cybersecurity standards are often surprisingly lax. Parties to an M&A transaction should carefully examine the level of cybersecurity of a merging counterpart or target company to mitigate the risks of inadequate cybersecurity.

Finally, Web sites may infringe trademarks not just by cybersquatting, but through non-visible data such as metatags. **Venture Tape Corp.** registered two trademarks in 1990 and spent the next 15 years developing their brand value. A competitor, **McGills Glass Warehouse**, appropriated Venture's trademarks by: (1) placing the trademarks in the metatags of the McGills Web site; and (2) placing the trademarks in white lettering on a white background. Although the incorporated trademarks were invisible to the Web site viewer, they had the effect of directing search engines to the McGills Web site when a search for Venture was executed. In *Venture Tape Corp. v. McGills Glass Warehouse*, Venture was awarded its attorneys fees and McGills' entire net profits from the infringing period.

Given the risks, parties to M&A transactions must take into account the "space" around a trademark when valuing a Web site, that is, they should consider the existence of infringing Web domains, non-infringing but similar or identical Web domains and the likelihood of consumer or brand confusion.

Proper data due diligence, and being aware of the data and electronic issues surrounding an M&A transaction, will sharply reduce risk, and help your company more accurately evaluate the likelihood of post-M&A success or failure.

Daniel B. Garrie is a managing member at EMI Capital LLC and a special master for electronic discovery for Alternative Resolution Centers. Yoav M. Griver is a partner at Zeichner, Ellman & Krause LLP. Anthony I. Giacobbe Jr. is of counsel with the firm. William M. O'Connor is a partner at Crowell & Moring LLP and chair of the firm's financial services group.

AS FEATURED ON



TheDeal.com (ISSN 1547-7584) is published by The Deal LLC.
© Copyright 2009 The Deal LLC. The Copyright Act of 1976 prohibits
the reproduction by any means of any portion of this publication
except with the permission of the publisher.

WWW.THEDEAL.COM