

 VOL. 30 | NO. 6
PUBLISHED BY TURNAROUND
MANAGEMENT ASSOCIATION

**JOURNAL OF
CORPORATE
RENEWAL**

TURNAROUND.ORG


JCR

JULY/AUG 2017

Supreme Court
Closes 'Backdoor'
Circumvention
of Bankruptcy
Priority Scheme

Generating Private Equity
Returns in the Face of
High Asset Pricing

Avoiding Costly Post-
Acquisition Disputes over
Portfolio Companies



**THE
ANATOMY**
of Investing
in Defaulted
Bonds & Loans

13613241
∞/-
10x/0.22

0.90/1.25 OIL 51
4x 10x 20x 40x



PRIVACY, CYBERSECURITY: What Private Equity, Restructuring Pros Need to Know

BY ERIK B. WEINICK, CIPP-US, OTTERBOURG P.C.

Target. Yahoo! PF Chang's. Home Depot. Sony.

These are but a handful of the headline-grabbing privacy and data breach incidents that have had direct negative business impacts on the affected companies. Organizations that ignore the reality of these incidents, as well as the growing body of applicable laws, regulations, and generally accepted business practices, do so at their peril.

Prudence therefore requires that organizations of all sizes and types develop, implement, and maintain appropriately reasonable systems for

ensuring the privacy and security of the information they receive, create, maintain, and/or transfer.

Firms involved in private equity and corporate restructuring are not immune from these concerns, and indeed, face certain unique issues.

As noted jurists Samuel Warren and Louis Brandeis wrote nearly 130 years ago, privacy is the "right to be left alone." [Harv. L. Rev. 4. 1890]. Privacy can include bodily privacy (the right to physical privacy), territorial privacy (the right to privacy in certain spaces, such as a person's home), information privacy (a person's right to keep

personal information private), and communications privacy (the right to privacy in communications).

Corporate privacy and cybersecurity professionals focus their work on information and communications privacy and are specifically concerned with what is known as "personally identifiable information" (PII). Although there is no official definition in the United States due to a lack of an overarching uniform federal regulatory scheme, PII is generally regarded as a person's name when combined with

continued on page 26

another identifier, such as a Social Security number, date of birth, bank account number, health records, or other sensitive information. The core legal question associated with PII is whether an organization is authorized to receive it, and if so, how it may use the information.

Privacy problems arise when an organization otherwise authorized to have PII uses it in an unauthorized or unanticipated manner. This can be illustrated by retailers and others that use data analytics, sometimes called big data, to predict, and even encourage, consumer behavior. More than a handful of companies have found themselves in hot water (if not legal, then at least with regard to their reputations) from their use of big data.

This improper use may be specifically prohibited by law, violate the privacy policies the companies provided to their customers, or simply fail the “creepy” test. One need look no further for an example of the creepy test than a retailer’s one-time practice of sending coupons for baby items to customers the company believed were expecting a child based upon their other purchases.

In contrast to privacy, cybersecurity focuses on the protection of electronic data and systems so that only authorized users have access. Broadly, a cybersecurity breach is defined by some as any unauthorized access to electronic systems and content (a more liberal definition) and by others as any unauthorized exfiltration of data (a more conservative definition).

Both privacy and cybersecurity concern the use and/or protection of information. However, privacy maintenance is not only concerned with protecting PII from theft but also with preventing its unauthorized use or misuse by those who are otherwise authorized to collect, maintain, and/or transfer the information. For example, a doctor’s sale or sharing of patient health information stored on his computer without patient consent may be a privacy violation, whereas cybercriminals hacking into the doctor’s computer to steal those same records would be a breach.

How Privacy, Cybersecurity Obligations Arise

Privacy and cybersecurity obligations

arise in two primary ways. The first is by statute or regulation. A common and well-known privacy regulatory example is the Health Information Portability and Accountability Act (HIPAA), which imposes certain requirements on those who handle patient healthcare records. An example of a cybersecurity regulation is the newly enacted regulations promulgated by New York’s Department of Financial Services, which mandate that all organizations operating under New York banking, insurance, or financial services laws, as well as their vendors and third-party service providers, must “assess [their] specific risk profile[s] and design a program that addresses its risks in a robust fashion.” [23 NYCRR 500].

Rules established by self-regulatory organizations, as well as recommendations or guidance published by industry associations, are also standards about which organizations should be mindful.

A second way privacy and/or cybersecurity obligations arise is by contract. Examples include the privacy policies posted to an electronic retailer’s website, which the consumer must acknowledge to complete a transaction, or security standards imposed on vendors. Many companies require their vendors to maintain a certain level of data security and subject them to compliance audits.

Particularly germane to consumer-facing organizations is the level of security these entities have promised their customers. The Federal Trade Commission (FTC) and other regulators have acted to enforce these promises on behalf of consumers. For example, in 2014, GMR Transcription Services Inc., which, as its name suggests, provides transcription services for healthcare providers, hospitals, and others, entered into a consent decree with the FTC under which it agreed to improve its information security practices, which, according to the FTC, were not as safe as the company represented them to be.

One of the best ways to ensure compliance with these obligations is to appoint a chief privacy officer (CPO) and/or chief information security officer (CISO). If the organization is not large enough to justify a full-time CPO or CISO, then it should empower someone of suitable authority within the organization to fill the

roles. At minimum, there should be one leading and authoritative voice within every organization when it comes to privacy and cybersecurity.

A CPO should be cognizant of the types of PII an organization maintains, how it does so, and what its obligations are with respect to the data. A CPO also should be involved in educating other members or employees of an organization as to their privacy responsibilities.

Likewise, a CISO should be responsible for overseeing and implementing an organization’s cybersecurity efforts. Written privacy and cybersecurity policies are not just helpful to this process, they are essential.

Private Equity, Restructuring Concerns

There are several privacy and cybersecurity issues that should be of particular concern to private equity and restructuring professionals. One is the manner in which electronic systems are interconnected throughout an organization. Systems may be connected from a portfolio company to the parent (vertically) and/or from portfolio company to portfolio company, either directly or through a common parent or operating company (horizontally).

If there are direct, or even indirect, connections between and among divisions, corporate affiliates, or commonly owned entities—which can serve an otherwise entirely legitimate business purpose, such as achieving economies of scale—cybercriminals can exploit security weaknesses at one portfolio company to access more valuable systems or data of a corporate sibling or parent. This is, of course, true not only across private equity-owned portfolio companies but also within a single monolithic organization.

And, it is not just cybercriminals who can cause problems. Companies often unnecessarily expose their data to misuse or mistakes when employees can access information that is not within the purview of their particular jobs.

To avoid data breaches from interconnected systems, organizations should employ multiple security measures. These include increasing the

Having the executive use two separate email addresses, one for holding company communications and another for portfolio company communications, may not only provide additional cybersecurity protection, but WARN Act insulation as well.

continued from page 26

level of security and decreasing access in proportion to the sensitivity of the data, such as through encryption and tiering; keeping connections across systems to a minimum; integrating newly acquired organizations in a careful manner and only after appropriately assessing and testing their security status; and educating employees about their front-line role in reducing cyber threats.

Members of the private equity and restructuring communities should also be aware of the risks presented by their frequent travel and use of temporary offices. Remote access systems should be secured using multifactor authentication, and personnel should be cognizant of the risks presented by public Wi-Fi, business center computers and printers, device screens that are easily viewed by others within the tight confines of an airplane, as well as unlocked phones that can be readily stolen from tablets in busy restaurants and bars.

Organizations may also wish to carefully evaluate their reliance on fingerprint identification as the sole means to unlock devices and/or access applications. See "That Fingerprint Sensor on Your Phone Is Not as Safe as You Think" by Vindu Goel, *New York Times*, April 10, 2017.

Putting aside cyber threats, interconnected electronic systems within the private equity environment can result in other liabilities, such as liability under the Worker Adjustment and Retraining Notification Act (WARN Act), 29 U.S.C. § 2101. The

WARN Act seeks to provide certain protections to workers in mass layoff situations, which often occur in connection with restructurings or bankruptcies, and is a popular tool for class action attorneys.

This should be a particular concern for private equity firms that employ certain individuals at the holding company level who "parachute in" to take on specific roles at portfolio level companies. For convenience and other legitimate and practical reasons, such executives may maintain only one email account (e.g., *aceexecutive@holdco.com*). However, in WARN Act litigation, plaintiffs often sue the monetarily flush holding company in addition to the bankrupt portfolio level company that was the direct employer of the terminated employees in the WARN Act class.

Therefore, having the executive use two separate email addresses, one for holding company communications and another for portfolio company communications, may not only provide additional cybersecurity protection, but WARN Act insulation as well. Such compartmentalization may serve as further evidence that the portfolio company's decision to terminate employees was not made at the holding company level and that the formal distinctions between them have been observed. Of course, from a cybersecurity perspective, the executive should, at minimum, have different passwords for each account.

A second issue derives from the commoditization of consumer data. In a restructuring, consumer data may be the only valuable asset

of the debtor. However, a debtor's ability to sell this information for use by the acquirer may be limited by, among other things, the debtor's prepetition consumer-facing privacy policy. Such was the case with the bankruptcy of True.com, a dating website, where the proposed sale of 43 million users' highly personal information was blocked because the site's privacy policy had promised not to sell or share the information without members' permission.

As a result of that case and others, companies have begun to structure their privacy policies to be ambiguous as to whether information will be sold or shared and/or they have "reserved" their right to make unilateral changes to the policy. It is therefore important that soon-to-be debtors recognize that their existing policy may limit their ability to monetize data.

If that is the case, they should consider whether to change the policy just before filing for bankruptcy protection. Thus far, such a last-minute change has not been found to be avoidable. However, there is no guarantee that a challenge to such a change may not succeed in the future.

Restructuring professionals should also be cognizant of the role of privacy ombudsmen as provided by 11 U.S.C. Section 332. Bankruptcy privacy ombudsmen are appointed to assist a Bankruptcy Court in considering the facts and circumstances surrounding a proposed sale or lease of PII under 11 U.S.C. Section 363, and they can present a strong challenge to the proposed sale or transfer of customer information by a debtor.

A third issue arises from the state in which investors, receivers, trustees, CROs, and/or foreclosing lenders may find a debtor or newly acquired company. When taking over a failing or failed firm (or any firm, for that matter), one may come into control of PII. One of the first steps that should be taken (if it was not already done during the due diligence process before the acquisition) is to assess what PII exists, what systems are in place to protect and manage it, and whether those systems are legally and technically sufficient.

It is possible that during a company's march toward bankruptcy and/or sale, privacy and cybersecurity controls were reduced to save cash. New management would be well-advised to remedy this to avoid any liability on its part and/or diminution in the value of the data (to the extent the data serves as collateral or an integral part of the new owner's business plan moving forward).

Prepare for the Worst

While the primary liabilities that have driven a company to bankruptcy, out-of-court restructuring, or acquisition are often staring retained professionals in the face, less apparent privacy and cybersecurity concerns can present hurdles to the completion and/or success of that acquisition or reorganization. Therefore, professionals advising debtors, creditors, and potential suitors should plan ahead of a crisis to identify, assess, and manage liabilities that may be attached to the sensitive data received, maintained, and transmitted by the debtor or target organization.

In addition, and unfortunately, the question of a data breach is not one of *if*, but of *when*. Therefore, in addition to preparing to deal with privacy and cybersecurity issues at debtors or targets, private equity and restructuring professionals must ensure that their own organizations build, implement, and maintain an overall privacy and cybersecurity program. While that task may seem overwhelming, it starts with an assessment of what type of information the organization has and what obligations attach to that information.

Next, the organization should consider obtaining or expanding its cyber insurance coverage and investigate retaining outside cyber incident response professionals (technical,



Erik B. Weinick is certified as a Privacy and Cybersecurity Professional (CIPP-US) by the International Association of Privacy Professionals (IAPP) and co-founded the Privacy & Cybersecurity practice group at Otterbourg P.C., which counsels firm clients on privacy and cybersecurity matters. In addition, Weinick is a member of the firm's Litigation practice group and regularly represents a diverse group of clients before state and federal courts, including Bankruptcy Courts; regulatory authorities; and alternative dispute resolution tribunals.

legal, and public relations) in advance of an incident. Conducted under the direction of outside counsel, a pre-incident evaluation may even be protected by attorney-client privilege from discovery during subsequent litigation initiated as a result of a breach. Even for organizations with in-house expertise in privacy and cybersecurity, tapping the outside perspective and experience of a

dedicated privacy and cybersecurity professional may be beneficial.

Finally, the organization should maintain vigilance and prepare for the inevitable breach by, among other things, conducting regular training, education, and exercises, and working collaboratively with vendors, customers, clients, and other business partners. ■

Unlock the



of your clients' equipment.

Lacking in cash flow but have equipment? Utica Leaseco can help improve your clients' position with a creative funding approach that gets challenging deals done, fast. They'll benefit with lease and loan solutions such as:

- Capital leases and sale/leaseback transactions
- Secured loans
- Debtor-in-possession financing

Contact us today!

586-726-5637 | info@uticaleaseco.com | www.uticaleaseco.com

