



PRIVACY & SECURITY LAW



REPORT

Reproduced with permission from Privacy & Security Law Report, 8 PVLR 27, 07/06/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Corporate Practices

Data Safeguarding in a Recession

Companies in today's economy must take stock of their information privacy and security practices to hedge against unnecessary liability. Issues of concern in this challenging economic environment include increased risk of exposure to data breaches brought on by unhappy or laid-off employees, unwanted liability due to inadequate or poorly enforced privacy and security policies, and restrictions on the use of personal information in the face of an eventual bankruptcy.

Testing the Roof: How an Economic Downturn Can Create Enhanced Risks to Corporate Information Security

By JOHN B. KENNEDY AND NATHAN C. DEE

I. Introduction

As every homeowner knows, the quality of the roofwork is never really known until the big rain comes, and the same principle holds true for corporate information security policies. In these times of

John B. Kennedy is a partner and Nathan C. Dee is an associate in the Information Technology and Intellectual Property practice group in the New York office of Dewey & LeBoeuf LLP.

economic recession, mass unemployment and corporate instability, it is increasingly important for companies to take stock of their information privacy and security practices and to hedge against unnecessary liability in the face of data breaches and inadequate information management. Layoffs, hiring and salary freezes, and a wide range of cost-cutting measures affecting technology and human resources may combine to weaken corporate security, which ultimately depends not only on technological measures but also on continuous administrative processes, employee awareness, and collective participation at all levels of the organization. When these latter elements weaken, whether through negligence or through deliberate or malicious acts or omissions by disgruntled or laid-off employees, information vulnerability increases. Under such conditions, some

employees may suddenly find themselves more willing to turn sensitive company information into personal opportunity.

This article examines some of the ways in which a downturn in economic conditions can create enhanced liability risks for companies that collect, store, use and/or disclose sensitive or proprietary information. Issues of concern in this challenging economic environment include increased risk of exposure to data breaches brought on by unhappy or laid-off employees, unwanted liability due to inadequate or poorly enforced privacy and security policies, and restrictions on the use of personal information in the face of an eventual bankruptcy. These and other issues involving information privacy and security in an economic recession are explored below.

Layoffs, hiring and salary freezes, and a wide range of cost-cutting measures affecting technology and human resources may combine to weaken corporate security.

II. Overview of Research/Studies

A number of recent studies have highlighted the increased risks to data security as a result of challenging economic conditions. One such study, conducted by the Ponemon Institute and sponsored by Symantec Corp., examines the risks posed by departing employees during periods of downsizing.¹ Most notably, the survey found that nearly 60 percent of respondents kept company data after leaving their former employer, which often included customer data, e-mail contact lists, employee records and other confidential business documents that could affect competitiveness and/or result in a data breach. Interestingly, the Ponemon survey cited employer oversight as a leading factor contributing to employee data theft; only 15 percent of companies conducted a review or performed an audit of the paper and/or electronic documents that employees were taking.² Moreover, 89 percent of respondents reported that their employer did not do an electronic scan of devices such as portable data-bearing equipment or USB memory sticks, and 24 percent reported that their access to company data continued long after they left their position.³ In short, companies had often failed to take proper steps to stop data theft in the face of downsizing or general employee attrition.

While the Ponemon study addressed data security risks specifically in the context of downsizing, a number of additional surveys have examined data breach and information security issues generally within the corporate environment. The 2008 Data Breach Investigations Report, conducted by Verizon, reported that although a majority of data breaches are caused by external sources, insider data breaches are generally much

larger in scope.⁴ Moreover, an annual survey produced by Deloitte Touche Tohmatsu (DTT) indicated that the current trend “is less on infrastructure and perimeter-strengthening and more on preventing information from being leaked internally,” as companies increasingly recognize that internal risks are a growing threat to information security.⁵ Thirty-six percent of respondents to the DTT survey indicated that internal personnel alone are the greatest concern with respect to information security systems.⁶ Notably, the Deloitte study also found that excessive access rights and a lack of segregation of duties allow some employees to circumvent control procedures.⁷ Finally, an additional 2008 study by the Ponemon Institute cited insider negligence as the highest cause of data breaches (over 88 percent of cases covered in the survey).⁸ Although these studies arrive at differing assessments of the extent and significance of internally-based threats to corporate information security, there is no doubt that such threats are real and are likely to be exacerbated in times of economic stress.

III. Key Areas of Risk for Employers

In light of the increased risks to data security in times of economic recession, it is especially important for businesses to be able to identify the primary risks posed and the potential ways of mitigating such risks. The discussion below outlines some notable increases in risk to data security and information privacy that a business may face in a down economy.

a. Inadequate or Poorly Enforced Employee Privacy, Computer and Internet Use Policies

It is important at all times for companies to maintain comprehensive and detailed information security policies and to enforce those policies consistently. In times of economic downturn, however, the prudence of such policies is even more apparent. Some recent cases demonstrate how inadequate or poorly enforced employee policies can lead to abuses of information security policies and litigation.

It is important at all times for companies to maintain comprehensive and detailed information security policies and to enforce those policies consistently.

One example of a privacy policy that went awry is found in *Quon v. Arch Wireless*. Employees of the City of Ontario, California were given two-way pagers on which they could send text-messages for employment

⁴ Wade H. Baker, C. David Hylender and J. Andrew Valentine, *2008 Data Breach Investigations Report: A Study Conducted by the Verizon Business RISK Team* (2008).

⁵ Deloitte Touche Tohmatsu, *Protecting What Matters: The 6th Annual Global Security Survey* (2009).

⁶ *Id.*, p. 39.

⁷ *Id.*, p. 21.

⁸ Ponemon Institute, LLC, *2008 Annual Study: Cost of a Data Breach* (February 2009) (8 PVL 233, 2/9/09).

¹ Ponemon Institute, LLC, *Data Loss Risks During Downsizing* (Published: Feb. 23, 2009) (8 PVL 363, 3/2/09).

² *Id.*, p. 2.

³ *Id.*, p. 4.

related purposes.⁹ The employees all signed an agreement acknowledging the city's "Computer Usage, Internet and E-mail Policy," which reserved the city's right to monitor activity on the pagers and stated that users should not have any expectation of privacy or confidentiality with respect to any communications sent over the pagers. However, the employees were also told informally by a supervisor that their text messages would not be audited or reviewed so long as they paid any applicable overage charges for going beyond their allowable number of characters. The U.S. Court of Appeals for the Ninth Circuit held that this "operational reality" of not reviewing text messages created a reasonable expectation of privacy for the city's employees, despite the fact that the city's written policy stated otherwise. Thus, *Quon* indicates the importance of having clear and concise monitoring policies, of ensuring that those policies are consistently enforced, and of clarifying any and all types of communications that will be monitored so that employees do not develop an expectation of privacy that trumps the terms of the employer's formal written policy.

In *Cardinal Health v. Adams*, a company successfully sued a former employee for violating the Stored Communications Act (SCA) by using a coworker's log-in information to read the coworker's e-mail and to spy on the activities of the company.¹⁰ The company benefited from the fact that it had taken away the former employee's access following his termination and had prominently stated on its log-on page that only employees were permitted to access the site. *Cardinal Health* illustrates the importance of addressing and limiting access rights granted to employees and of being diligent in removing those rights promptly upon an employee's termination.

Another area of concern for employers is the increased use of portable devices and removable media such as USB storage devices and mp3 players. The proliferation of such devices in the work environment has made it imperative for companies to address them in corporate information policies and, where such devices are permitted, to have published rules for monitoring the devices and for specifying what data can be stored on them. In *Teksystems v. Modis*, a company successfully stated a Computer Fraud and Abuse Act (CFAA) claim against a former employee who downloaded trade secrets and confidential client information onto an external hard drive after accepting a position with the company's competitor.¹¹ The court held that an employee who accesses a computer in breach of his duty of loyalty to his employer loses any authorization to access the computer and thus violates the CFAA. In a similar case, a company prevailed on its CFAA claim

against a former employee who used a software erasure program to permanently delete business and contact lists along with client leads from his company-issued laptop.¹² The court denied the employee's motion to dismiss the CFAA claim and noted that the employee lost his authorization to access the data once he decided to terminate his employment and form a competing business.

However, a number of courts have taken a different view with respect to the issue of unauthorized access under the CFAA. For example, the U.S. District Court for the District of Arizona held that a former employee's acquisition of confidential information prior to resigning from employment was not "without authorization," as the employee was initially authorized to access the computer as well as view the data he subsequently e-mailed to himself.¹³ Similarly, the U.S. District Court for the Southern District of Texas recently held that employees who copied their employer's customer and vendor lists on their last day of work (and subsequently used them to start a competing business) could not be sued under the CFAA because they were properly authorized to access the data in connection with their employment.¹⁴

b. Other Risks Associated with Surveillance and/or Electronic Monitoring of Employees

Quon and other cases indicate that a comprehensive and consistently-enforced workplace monitoring policy is an indispensable tool to safeguard and detect misappropriation of sensitive data. In *Hilderman v. Enea TekSci*, for example, an employer was able to detect a former employee's e-mail disclosures of confidential information by searching his company-issued laptop.¹⁵ The former employee's motion for summary judgment on the issue of invasion of privacy was denied. One significant take-away from the *Hilderman* case was the court's ruling that an employee's storage of personal e-mails on the hard drive of a company-issued laptop did not constitute "electronic storage" within the meaning of the SCA because such e-mails were not in "temporary, intermediate storage" on an ISP's server or stored "by an electronic communication service for purposes of backup protection."¹⁶ Thus, personal e-mails stored on company laptops do not subject the employer to the privacy restrictions associated with the SCA. The *Hilderman* case again highlights the importance of a comprehensive monitoring policy that includes policies with respect to monitoring company-issued laptops and personal e-mails stored on such laptops.

¹² *Alliance Int'l Inc. v. Todd*, 2008 WL 2859095 (E.D.N.C. 2008) (7 PVL 1156, 8/4/08).

¹³ *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008) (7 PVL 390, 3/17/08).

¹⁴ *Bridal Expo Inc. v. Van Florestein*, 2009 U.S. Dist. LEXIS 7388 (S.D. Tex. 2009) (8 PVL 275, 2/16/09).

¹⁵ *Hilderman v. Enea TekSci Inc.*, 551 F. Supp. 2d 1183 (S.D. Cal. 2008) (7 PVL 420, 3/24/08).

¹⁶ *Id.* at 1204.

⁹ *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008) (7 PVL 938, 6/23/08).

¹⁰ *Cardinal Health 414 Inc. v. Adams*, 582 F. Supp. 2d 967 (D. Tenn. 2008) (7 PVL 1580, 11/3/08).

¹¹ *Teksystems Inc. v. Modis Inc.*, 2008 WL 5155720 (N.D. Ill. 2008).

Companies that monitor employees' instant messaging chats or telephone calls need to explicitly bring such monitoring practices to the attention of the employees and obtain such employees' express consent to do the same.

Nevertheless, employers should be aware of the pitfalls associated with real-time monitoring and surveillance of employee communications. Companies that monitor employees' instant messaging chats or telephone calls need to explicitly bring such monitoring practices to the attention of the employees and obtain such employees' express consent to do the same. In *Garza v. Bexar Metropolitan Water District*, a governmental entity was held to be in violation of the Federal Wiretap Act for monitoring and intercepting an employee's business and personal calls.¹⁷ Noting that the employer had no policy that informed employees that their telephone calls were subject to interception, the court denied the employer's motion to dismiss. Moreover, although state laws differ on whether the consent of all parties is required to record a conversation (e.g., California) or whether just one party's consent is required (e.g., Georgia), at least one court has held that companies operating in a one-party consent state may be subject to the higher standards of an all-party consent state if they regularly receive calls from residents of that state.¹⁸

In view of the current state of the economy, fact patterns such as these are likely to recur. Companies may want to revisit the effectiveness of their exit-interview processes and related termination procedures to identify employees who have had access to sensitive data and to assure that access privileges are promptly and securely terminated. Companies should also seriously consider banning or disabling the use of removable media (USB drives, etc.) on their computers. Most importantly, companies should have a comprehensive monitoring policy in place which provides adequate notice to employees, as well as any other individuals whose conversations may be monitored or recorded.

c. Risks Associated with Employee Investigations

Recent cases have also highlighted certain risks associated with conducting background checks on current or potential employees. In *Beverly v. Wal-Mart*, for example, Wal-Mart hired an independent third party (ChoicePoint) to conduct a background check on a potential employee.¹⁹ ChoicePoint's report contained inaccurate information about the potential employee, and Wal-Mart allegedly took adverse action by denying him

employment without first offering him an opportunity to correct the faulty information. The court denied the defendant's motion for summary judgment in connection with the plaintiff's claims that Wal-Mart violated the Fair Credit Reporting Act (FCRA). Moreover, in *EEOC v. Video Only*, certain employees of a video store chain filed a complaint with the store's corporate headquarters alleging discrimination by the store's manager.²⁰ In response to the complaint, a private investigator hired by senior executives at the company began contacting friends and family of the employees and asking personal questions about the employees' backgrounds. The court held that Video Only violated numerous sections of the FCRA, including by failing to notify the employees that an investigative consumer report would be obtained and by seeking a report for impermissible purposes. These cases demonstrate the need to be aware of the obligations and requirements under the FCRA in connection with conducting background checks on current and potential employees in order to avoid unnecessary liability.

d. Heightened Risk of Employee-Caused Data Breaches

In addition to the risks posed by employee monitoring and abuse of company information security policies, companies are dealing with a rise in seemingly-intentional data breaches involving actions by employees. In May 2009, for example, the California Department of Public Health fined Kaiser Permanente's Bellflower Hospital \$250,000 in connection with a data breach involving a number of employees who inappropriately accessed the medical records of Nadya Suleman, the woman who gave birth to octuplets in January 2009. In another example, a 22-year veteran employee of the New York State Department of Taxation and Finance was arrested and charged with multiple felonies after allegedly stealing the personal identifying information (including Social Security numbers) of over 2,000 taxpayers.²¹ Moreover, in Japan, a deputy general manager of Mitsubishi UFJ Securities allegedly stole personal information on the company's 1.5 million clients and sold it to various marketing firms.²² The steady flow of reported data breaches, coupled with survey findings of the kind noted at the beginning of this article, suggest that the ability to monetize corporate information assets such as customer data has on at least some occasions proved too tempting for certain employees.

Whether employees' motivations behind these reported incidents are driven by economic events is debatable, but it is certain that the consequences of their actions can lead to significant liabilities for their employers, including the costs of complying with data breach notification laws and in some cases civil penalties imposed by state regulators. Accordingly, companies should incorporate appropriate hiring, training, monitoring and termination practices in their information security policies. Moreover, the increasing ability of employees to work from remote locations through

¹⁷ *Garza v. Bexar Metro. Water Dist.*, 2009 WL 563222 (W.D. Tex. 2009).

¹⁸ *Kearney v. Solomon Smith Barney Inc.*, 39 Cal. 4th 95 (2006) (5 PVL 981, 7/17/06).

¹⁹ *Beverly v. Wal-Mart Stores Inc.*, 2008 U.S. Dist. LEXIS 2266 (E.D. Va. Jan. 11, 2008).

²⁰ *EEOC v. Video Only Inc.*, 2008 U.S. Dist. LEXIS 46094 (Ore. 2008).

²¹ *New York v. Healey*, Troy City Ct., No. 095062, indictment 4/21/09 (8 PVL 628, 4/27/09).

²² See: <http://www.forbes.com/feeds/afx/2009/04/08/afx6268208.html> (see related report in this issue).

the use of telecommunications and remote access creates even greater risks that sensitive and proprietary information will remain on remote user devices after the employee has left the company. Company policies should clearly address and limit the use of remote devices and incorporate periodic inspections and audits of such devices (especially prior to an employee's departure) to ensure that company information is not being stored thereon.

e. Sales and Transfers of Personally Identifiable Information in Business Closings, Bankruptcy Sales and Liquidations

In addition to the heightened data loss risks associated with fired or disaffected employees, businesses that are forced into asset sales, divestitures or insolvency must reckon with the lawful disposition of valuable customer data, which in some cases may be among the most material assets of the business. In non-bankruptcy sales, the transferability of non-public personal customer information will depend primarily on the previous promises a business has made to its customers. Categorical privacy policy promises never to sell or transfer customer data may prove problematic in an asset sale that includes customer databases. Although the law in this area is limited and unsettled,²³ companies that seek to sell customer data in an asset sale and have represented to their customers that no such transfer of personal information will occur without their consent should consider opt-out or opt-in mechanisms in connection with the sale to mitigate the risk of civil litigation or regulatory complaints.

The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA) created restrictions on the sale or transfer of "personally identifiable information" (PII) as part of a Section 363 asset sale in bankruptcy. Almost all companies that collect consumers' PII have a privacy policy in place with respect to the sharing of PII, as mandated by the Gramm-Leach-Bliley Act and other regulations. BAPCPA's changes to Section 363(b)(1) prohibit a debtor from selling or leasing to nonaffiliated entities any PII in its possession as part of a Section 363 sale, unless (i) such sale or lease is con-

sistent with the debtor's privacy policy or (ii) after appointment of a Consumer Privacy Ombudsman (CPO), such sale or lease is approved by the courts.²⁴

The appointment of a CPO is not necessary where the debtor is able to structure the transfer of PII to comply with its privacy policy (for example, by allowing consumers to opt out of the transfer). Additionally, the foregoing provisions only apply if the transfer of PII is outside the ordinary course of business. Thus, companies that regularly engage in transfers of PII are not prohibited from doing so in a Section 363 sale. The appointment of a CPO becomes a necessity when a company either has no privacy policy or if its privacy policy prohibits the transfer of PII. In most cases, the appointment of a CPO generally results in a revision of the privacy policy to allow for the transfer of PII and is usually accompanied by an order requiring companies to give consumers an opportunity to opt out of the proposed transfer.²⁵ Companies should also keep in mind that in addition to the CPO provisions of the Bankruptcy Code, there are other statutes that restrict transfers of PII: the Children's Online Privacy Protection Act regulates collection of PII from children;²⁶ the Health Insurance Portability and Accountability Act regulates the use and collection PII in electronic medical records;²⁷ the Fair Credit Reporting Act regulates the use and collection of personal financial information;²⁸ and GLB regulates collection and use of PII by financial institutions.

IV. Conclusion

The stresses of a significantly down economy are felt everywhere, and corporate information security is no exception. No business wants to compound the challenges of a harsh economic climate with preventable losses and disputes arising out of missteps in corporate information management practices. Most of the problems for businesses highlighted in this discussion can be mitigated by following well-established information security practices, even if it means fixing the roof in the rain.

²⁴ 11 U.S.C. § 363(b)(1).

²⁵ *JS Mktg. and Commc'ns Inc.*, Case No. 05-65426-11 (Bankr. D. Mont. 2006); *In re Refco Inc.*, Case No. 05-60006 (Bankr. S.D.N.Y. 2006); *In re Three A's Holdings LLC*, Case No. 06-10886 (Bankr. D. Del. 2006); *In re Engaging and Empowering Citizenship Inc.*, Case No. 02-BKC-28175-CGC (Bankr. D. Ariz. 2006); *In re Bodies in Motion Inc.*, Case No. 06-10931 (Bankr. C.D. Cal. 2006); *In re W. Med. Inc.*, Case No. 06-01784 (Bankr. D. Ariz. 2006); *In re Faxtons Inc.*, Case No. 07-24496 (Bankr. D. N.J. 2007); *In re R.J. Gators Inc.*, Case No. 07-14954 (Bankr. S.D. Fla. 2007); *In re Storehouse Inc.*, Case No. 06-11144 (Bankr. E.D. Va. 2007); *In re Tweeter Home Entm't Group Inc.*, Case No. 07-10787 (Bankr. D. Del. 2007); *In re Chrysler LLC*, 2009 WL 1360869 (Bankr. S.D.N.Y. 2009).

²⁶ 15 U.S.C. §§ 6501 *et seq.*

²⁷ 42 U.S.C. § 1320d.

²⁸ 15 U.S.C. § 1681.

²³ See, e.g., *In the Matter of Gateway Learning Corp.*, FTC File No. 042-3047 (2004) (Gateway Learning entered into a consent decree with the FTC in connection with charges that the company sold personal customer information to target marketers without disclosing such practices in the company's privacy policy) (3 PVL 803, 7/12/04); Press Release, Office of the Attorney General of New York (Jan. 11, 2001), available at: http://www.oag.state.ny.us/media_center/2001/jan/jan11a_01.html (Internet toy distributor Toysmart.com entered into a settlement with the New York Attorney General prohibiting the company from selling its customer lists and databases as part of the sale of its assets in bankruptcy proceedings).