VEDDER PRICE

eDiscovery Update

February 2007

DATA SECURITY BREACH NOTIFICATION

Information management extends beyond eDiscovery and e-mail archiving. Indeed, in 2005, over 80 companies, universities, hospitals and government entities suffered security breaches that compromised various personal and financial data. The majority of these breaches affected tens of thousands of individuals, with some affecting millions. The largest, involving a company called CardSystems, resulted in the disclosure of data of approximately 40 million people.

The loss of customer data can result from negligence, hackers or theft. By way of example, in February 2005, ChoicePoint, a company that collects and compiles personal and financial information, disclosed that it had been a victim of a security breach. Criminals gained access to ChoicePoint's database by signing up for the company's service using stolen credit cards and posing as legitimate businesses. The criminals then created up to 50 different accounts to search the files of up to 145,000 people nationwide.

These security breaches have prompted states to introduce legislation requiring organizations to disclose to consumers security breaches involving personal information. As of January 9, 2007, 35 states have enacted legislation requiring companies to disclose data security breaches concerning personal information.[1]

The legislation typically requires notice-triggering information to have been compromised before requiring notification. In some states, the legislation requires an organization to notify individuals of a security breach when personal information has been materially compromised. In other states, the legislation requires notification when there is a likelihood of harm to the consumer due to the security breach. Some states, such as California, require notification when personal information has been or is reasonably believed to have been acquired by an unauthorized person. The purpose of notifying individuals is to enable them to take actions to protect themselves against identity theft or other possible harm.

When determining whether to notify individuals of a security breach, consider whether the information is in the physical possession and control of an unauthorized person (such as in the case of a lost or stolen computer or other device containing notice-triggering information). Also consider whether the information has been downloaded or copied and whether the information was used by an unauthorized person to establish fraudulent accounts or for identity theft. When notification would allow individuals to take action to protect themselves from possible harm, consider providing notice even if the compromised information is not notice-triggering information. However, keep in mind that continual notification of non-notice-triggering information can make many individuals complacent, which minimizes the effectiveness of the notice.

In This Issue

Notify the affected individuals in the most expedient and timely way possible after discovery of an incident involving unauthorized access to notice-triggering information. Take steps to contain and control the systems affected by the breach and conduct a preliminary internal assessment of the scope of the breach. Once you have determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person, notify affected individuals within 10 business days unless law enforcement authorities tell you that providing notice at that time would impede their investigation.

When notifying individuals, include a general description of what happened, the type of personal information that was compromised, what has been done to protect the individuals' personal information from further unauthorized acquisition, what your organization will do to assist individuals and information to help individuals protect themselves from identity theft (including contact information for the three reporting agencies).

Make sure that the notice is clear, concise and conspicuous. Use clear, simple language, guiding subheadings, and plenty of white space in the layout. Avoid using jargon or technical language. In addition, avoid using a standard format, which may result in complacency toward the notice.

Send the notice by first-class mail. Alternatively, consider sending notice by e-mail if you normally communicate with the affected individuals by e-mail and have received their prior consent to that form of notification. If you cannot identify the specific individuals whose notice-triggering information was acquired, notify all those in groups likely to have been affected. When a large number of individuals have been affected (*e.g.*, 500,000), or you do not have adequate contact information on those affected, provide notice using public channels. Post the notice conspicuously on your website, notify through major statewide media (television, radio and print), and send notice by e-mail to any affected party whose e-mail address you have.

If you believe that the incident may involve illegal activities, report it to the appropriate law enforcement agencies. When contacting law enforcement agencies, inform them that you intend to notify affected individuals within 10 business days. If a law enforcement agency tells you that giving notice within 10 days would impede the criminal investigation, ask them to inform you as soon as you can notify the affected individuals. It should not be necessary for a law enforcement agency to complete an investigation before notification can be given. Upon notification from the law enforcement agency, send notice to affected individuals immediately.

These recommendations can serve as guidelines for organizations to assist them in providing timely and helpful information to individuals whose personal information has been compromised while in the organization's care. However, these recommendations do not include all the practices that should be observed. Organizations should periodically review and update their own situation to ensure compliance with the laws and principles of privacy protection. It should be recognized that specific or unique considerations, including compliance with other laws, may make some of these practices inappropriate for some organizations.

Managing Risks Associated with Employee Blogs

A blog, short for "weblog," is an online journal where the author can share his or her thoughts and opinions with the millions of people who surf the Internet each day. To capitalize on the rapid rise in popularity of blogs as a form of new media, many of the nation's leading companies have begun to publish official corporate blogs as a means to humanize the company, reach customers and address critics in a personal and informal way.[2] As companies are enthusiastically joining the "blogosphere," they should be mindful that their employees are also turning to blogging as a form of self-expression, and that the content of their

employee's private blogs may have legal and financial ramifications for the company.[3]

An employee's personal blog may chronicle all aspects of his or her life, including work. Where employees use a public forum, such as blogging, to share their thoughts on corporate policies or business decisions of their employers, there is a danger that they will disclose confidential business information or trade secrets. Where an employee's blog contains inappropriate or harassing comments about another employee, a company may be vulnerable to claims for sexual harassment and hostile work environment.[4] Companies also face a growing threat of defamation claims where the employee's private blog contains defamatory comments on topics within the scope of the employee's employment or authority.

In light of these dangers, employers have begun to discipline or terminate employees for the content of their personal blogs.[5] However, prior to making the decision to discipline or terminate an employee for the content of his or her personal blog, an employer should consult with an attorney to make sure their actions will not run afoul of the law. In particular, a company should examine whether their actions may be construed as punishing an employee for engaging in a protected activity such as, *inter alia*, the organization of union activity, or the discussion of wages, hours, and other terms of employment.[6] Additionally, a company should consider the negative impact that disciplining an employee for their private, off-duty activities may have on employee morale and on the company's public image.

In order to inform their employees of the possible dangers that their off-duty blogging may pose to their employer as well as to their own job security, an employer should formulate a company policy specifically addressing off-duty Internet usage. In general, an off-duty Internet usage policy should remind employees that:

- They are personally responsible for the content of their blogs and other personal Internet communications;
- The content of their off-duty Internet communications should comport with corporate policies, including those prohibiting the disclosure of the company's confidential information and trade secrets;
- Their communications should abide by all laws, in particular those concerning the disclosure of financial information; and
- They may not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful or embarrassing to any other person or entity.

By adopting a comprehensive off-duty Internet usage policy, a company puts its employees on notice of the standards that apply to blog postings and, accordingly, a company may begin to minimize the risks that stem from an employee's private blog.

Vedder Price's attorneys have developed a premier national reputation and considerable experience in information management. Our Records Management Solutions and eDiscovery practice group is comprised of attorneys dedicated to enabling our clients to develop customized, yet comprehensive, solutions to minimize litigation risks and costs, increase records management efficiency and achieve compliance with all applicable governmental regulations and statutes as well as industry best practices.

The editors of eDiscovery Update, Bruce A. Radke and Timothy J. Carroll, express their gratitude to Michael J. Waters and Laurel A. Dearborn for their assistance in preparing this article.

[1] *See* State Security Breach Notification Laws, *http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm*.

[2] There are about 1.2 million new blogs created each day. *http://www.technorati.com/weblog/2006/02/81.html*. General Motors, Boeing, Microsoft, and Sun Microsystems each have developed an official or quasi-official corporate blog. William M. Bulkeley, Technology *(A Special Report); The Inside View: Employee blogs can put a human face on companies; But that's not always a good thing*, WALL ST. J., Apr. 3, 2006, at R7.

[3] For example, in 2004, Delta Airlines learned that one of its flight attendants had posted suggestive photos of herself in her Delta Airlines uniform on her personal blog. Delta terminated her for the unauthorized use of Delta branding, and she subsequently brought an EEO charge against Delta. *See* Jo Twist, *US Blogger Fired by her Airline*, BBC NEWS, Nov. 3, 2004, available at *http://news.bbc.co.uk/1/technology/3974081.stm*.

[4] The court in *Blakey v. Continental Airlines*, 164 N.J. 38 (2000), held that an employer was liable for a claim of hostile work environment where it had reason to know that derogatory comments posted on an employee's private blog about another employee were part of a pattern of harassment in the workplace.

[5] A 2006 survey done by the American Management Association and ePolicy Institute found that 2% of employers have fired workers for posting offensive content in their blogs. M.P. McQueen, *Workers' Terminations for Computer Misuse Rise*, WALL ST. J., July 15, 2006, at B4.

[6] The National Labor Relations Act ("NLRA"), 29 U.S.C §§157, 158 (2006), prohibits an employer from firing an employee for urging other employees to complain about a particular employment practice. Additionally, in *Konop v. Hawaiian Airlines, Inc.*, the Ninth Circuit Court of Appeals, relying on NLRA precedent, held that an employee's critical comments regarding labor concessions sought by his employer were protected as concerted activity for the purpose of collective bargaining under the Railway Labor Act. 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003). Employers should also be mindful of other labor laws such as federal and state whistleblower statutes, as well as laws protecting privacy and free speech. For example, California labor laws prohibit an employer from interfering with its employees' political activities. Cal. Labor Code §§ 1101-02 (2006).

VEDDER, PRICE, KAUFMAN & KAMMHOLZ, P.C.

This bulletin is published by the law firm of Vedder, Price, Kaufman & Kammholz, P.C. It is intended to keep our clients and interested parties informed on recent legal developments. It is not a substitute for professional advice.

Vedder Price is a national full-service law firm with approximately 235 attorneys in Chicago, New York, Washington, D.C. and Roseland, New Jersey. Please contact your Vedder Price attorney with any questions or if you need any assistance.

Chicago
222 North LaSalle Street
Chicago, Illinois 60601
312-609-7500
Fax: 312-609-5005

New York
805 Third Avenue
New York, New York 10022
212-407-7700
Fax: 212-407-7799

Washington, D.C.
875 15th Street, N.W., Suite 725
Washington, D.C. 20005
202-312-3320
Fax: 202-312-3322

New Jersey
Five Becker Farm Road
Roseland, New Jersey 07068
973-597-1100
Fax: 973-597-9607

www.vedderprice.com