TIMOTHY J. CARROLL, BRUCE A. RADKE & MICHAEL J. WATERS

You must prepare for a data security breach

Companies have developed new ways to create, store, access, use and ***lose*** data. Indeed, since January 2005, the Privacy Rights Clearinghouse has reported that more than 1,000 data breaches have occurred, involving more than 220 million records. In reality, the number of actual data breaches is much higher, given that many incidents are not reported. Notably, in the first quarter of 2008, 167 data breaches have been reported, involving 8.3 million financial and consumer records.

A data breach or loss can occur in a variety of ways:

- An executive loses a laptop;
- A hacker accesses a Company's computer storage system;
- A rogue employee steals his employer's confidential data;
- A Company improperly disposes of its records;
- A third party responsible for maintaining, transporting, or processing data is negligent in its handling; and
- Simple human error.

Significant data breaches have occurred in every industry and have hit manufacturers such as SAIC, who in July 2007, may have disclosed the personal information of more than half a million individuals because it did not encrypt data transmitted online. In the same month, Pfizer, had the identities of 17,000 current and former employees compromised when an employee's spouse installed unauthorized file-sharing software on a company laptop on which this data was stored.

Best Buy's $54 million lost laptop

Articles and reports of privacy litigation have discussed the problems and damages awards that companies face when they are the victims of security breaches involving the disclosure of customer or employee personally identifying information ("PII"). Typically, these issues arise in the context of large-scale security breaches, such as those affecting SAIC and Pfizer. However, a recent event involving Best Buy serves as a reminder that such security breach issues are not limited to large-scale breaches.

In May of last year, Raelyn Campbell left her malfunctioning year-old laptop at a Washington D.C. area Best Buy for routine repairs under a service contract, but Best Buy failed to return the laptop. For months, Ms. Campbell sought information regarding the whereabouts of her computer, and for months, Best Buy equivocated. Eventually, Best Buy confirmed what Ms. Campbell already suspected, that it had lost her computer.

With a corporation as big as Best Buy, thefts are inevitable, and equipment will occasionally be lost. Thus, at first blush, the loss of a single laptop may not seem like a big deal. However, when companies do not have a predetermined policy in place for responding to such incidents, they can unwittingly subject themselves to far more civil liability and negative publicity than one might expect.

On November 16, 2007, Ms. Campbell filed a lawsuit against Best Buy in Washington Superior Court,

see **SECURITY BREACH** *page 24*

Timothy J. Carroll can be reached at 312-609-7709 or tcarroll@vedderprice.com; **Bruce A. Radke** can be reached at 312-609-7689 or bradke@vedderprice.com; and **Michael J. Waters** can be reached at 312-609-7726 or mwaters@vedderprice.com. They are all members of Vedder Price's privacy litigation and counseling team.

SECURITY BREACH

Cont. from page 19

seeking $54 million in damages. In her complaint, Ms. Campbell alleges that Geeksquad (Best Buy's computer service subsidiary) and Best Buy customer service employees created a false record of her computer within their system and lied about its repair status and location.

Ms. Campbell also alleges that, in losing her computer, Best Buy put her PII at risk, as the computer contained information such as her social security number, drivers license number and credit card information. Ms. Campbell additionally alleges that Best Buy compounded the problem by waiting months before advising her that the computer was missing, and that her personal information might be in the hands of others. More specifically, Ms. Campbell is alleging that Best Buy violated the Washington D.C. Consumer Protection Procedures Act and the Washington D.C. Consumer Personal Information Security Breach Notification Act.

Best Buy's actions, as characterized by Ms. Campbell, could constitute unlawful trade practices under the Consumer Protection Procedures Act. Perhaps even more problematic for Best Buy are its alleged violations of the Consumer Personal Information Security Breach Notification Act, the stated purpose of which is to "ensure that consumers are notified when electronically-stored personal information is compromised in a way that increases the risk of identity theft, to create a private right of action for consumers harmed by a violation of the notification requirement, and to provide for enforcement by the Attorney General." Given that personal information identified under the Act, such as social security numbers, driver's license numbers or credit card information, would be stored on a customer's personal computer, there is a strong likelihood that the Act imposed upon Best Buy a duty to notify Ms. Campbell immediately upon discovering that her computer was missing.

Specifically, the Act requires that "[a]ny person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery." Beyond the cost of defending such a suit and any adverse judgment for actual damages, the Act also authorizes a plaintiff to recover "the costs of the action and reasonable attorney's fees."

While personal information security breach-related issues generally arise when large databases containing the personal information of thousands of people are compromised, this case demonstrates the need to be prepared even for a breach involving a single consumer. Had Best Buy had a predetermined policy in place in advance of this incident (or followed any pre-existing policy it may have had in place), it might have forestalled any potential liability. In fact, the Consumer Personal Information Security Breach Notification Act specifically protects businesses that have such a policy in place: "a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this subchapter shall be deemed to be in compliance with the notification requirements of this section if the person or business provides notice, in accordance with its policies, reasonably calculated to give actual notice to persons to whom notice is otherwise required to be given under this subchapter."

Although it is unlikely Ms. Campbell will ever receive the $54 million she seeks, Best Buy has opened itself up to the possibility of a judgment that would be significant to most companies, not to mention damaging to its reputation. Ms. Campbell has already appeared on the *Today Show,* and her story has been reported by numerous media outlets. This case thus highlights the need for companies handling sensitive personal information to maintain predetermined and up to date plans in the event of a security breach, and to remember that such plans should be followed even where only a single person's personal identification information is at issue. In addition to protecting themselves by enacting a company policy on security breach notification procedures, companies should take steps to lessen the likelihood of a security breach in the first instance.

Companies may be able to avoid liability in the event of a breach

One area in which corporate defendants have been able to successfully defend themselves in personal information security breach cases is in the area of damages, as multiple courts have ruled in defendant's favor where plaintiffs have been unable to demonstrate the existence of damages. A recent California Federal appellate decision, *Stollenwerk v. Tri-West Health Care Alliance,* sheds further light on when alleged damages are sufficient to withstand a motion for summary judgment.

In *Stollenwerk,* the plaintiffs brought claims against Tri-West Health Care Alliance after their personal information was lost during a December 2002 burglary at Tri-West's headquarters. The plaintiffs argued that Tri-West did not take sufficient steps to protect their personal information. After the break-in, one plaintiff became the victim of identity theft. Although there was no direct evidence that the identity theft resulted from the burglary, the court held that there was sufficient circumstantial evidence to allow the plaintiff's case to proceed to trial. However, with respect to the other plaintiffs, who had their personal information stolen but were not victims of identity theft, the court held that any damage they sustained, in the form of having to purchase credit monitoring insurance, was not sufficient, and the court did not allow their case to proceed to trial.

The *Stollenwerk* decision is both good and bad for defendants in personal information security breach cases. On one hand, to the extent that credit monitoring is not a recoverable cost, it becomes difficult for consumer plaintiffs to maintain large class action lawsuits. (This is also true where corporations suffering a security breach offer credit monitor-

see **SECURITY BREACH** *page 25*

SECURITY BREACH

Cont. from page 24

ing to affected consumers.) On the other hand, the Court did create openings for some plaintiffs to make it past the summary judgment stage of litigation, even where there is no direct evidence of a connection between the security breach and subsequent identity theft.

Steps to take to lessen the likelihood of a privacy breach

As illustrated above, all companies must take proactive steps to mitigate the likelihood of a privacy incident. Indeed, 43 States (and counting) have enacted data security breach notification laws, so that if an incident occurs, your company must understand what constitutes a violation, when a notice of data security breach is required, and whether it must alert Federal, State or local authorities. Additionally, your company should strive to:

- Develop Data Security Policies and Response Protocols in the event of a data security breach;
- Involve your company's compliance, human resources, information security and inside and outside legal teams in the development of your company's Data Security Policies and Response Protocols;
- Understand how Data Security Notification Laws will impact your Company's response and guide your company's policies;
- Develop a policy on employee blogging, which poses the risk of employees defaming fellow employees, divulging proprietary and confidential information, and violating other company policies;
- Identify patterns and activities that present "red flags" indicating possible identity theft;
- Respond appropriately and swiftly, should a "red flag" arise;
- Review agreements with vendors and third-parties who maintain PII regarding your employees and customers; and
- Document steps taken to respond to a data security event in order to demonstrate compliance with applicable laws and regulations. ■

Vedder Price's privacy litigation team has represented large companies and manufacturers and distributors in mitigating the risks associated with data theft, complying with applicable laws and regulations, and in litigation involving the loss and/or wrongful use of personally identifying information. For further information on this article or Vedder Price's privacy litigation and counseling team, please contact one of the authors listed at the bottom of page 19.

Reprinted with permission from:

The Illinois Manufacturer

Summer, 2008 issue

The Illinois Manufacturer is the official publication of the Illinois Manufacturers' Association (IMA)
220 East Adams Street • Springfield, Illinois 62701 • 217-522-1240 • Fax: 217-522-2367
1211 West 22nd Street • Suite 620 • Oak Brook, Illinois 60523 • 630-368-5300 • Fax: 630-218-7467
Visit http://www.ima-net.org/library/tim.cfm for editorial and advertising information