Companies Must Prepare for Data Theft

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

The authors discuss steps that companies can take to mitigate the risks of, or damages caused by, a security breach.

The need for companies to have a predetermined plan in place in the event of grand-scale data theft has been highlighted by recent events. On August 17, 2007, the job-search web site Monster.com discovered that invaders had stolen the personal information of approximately 1.3 million of its users.

Hackers infiltrated Monster's password-protected resume library using credentials stolen from clients. Monster was informed of the issue by the Internet security company Symantec. Within days Monster's security team had identified the rogue servers, and the web-hosting company shut them down by the morning of August 21.

Based on the security team's review, the breach was limited to names, addresses, phone numbers, and e-mail addresses. However, on August 21, Symantec reported that it had discovered copies of scam e-mails that the hackers used in their attempt to obtain more meaningful information such as financial data. The hackers were posing as official recruiters acting through the web site and asking recipients to provide information such as bank account numbers. These e-mails also contained links that could infect a recipient's computer with dangerous software if clicked on.

Monster did not begin to inform users about the data theft until

The authors, members of Vedder Price's privacy litigation team, can be reached at tcarroll@vedderprice.com, bradke@vedderprice.com, and mwaters@vedderprice.com, respectively.

Published in the February 2008 issue of Privacy & Data Security Law Journal.

August 22, five days after it had initially discovered the breach and a day after Symantec issued its report. While this might seem like a reasonable delay, it is unclear whether Monster's response was timely enough to avoid liability.

Monster is not alone in falling victim to these crimes. On June 1, 2007, 17,000 past and present employees of Pfizer received a letter advising them of the unauthorized disclosure of their names, Social Security numbers, and, in some instances, addresses, and bonus information to one or more third parties. On June 29, a class action was commenced on behalf of these employees alleging that Pfizer had breached fiduciary duties owed to the class members and violated Louisiana's Database Security Breach Notification Law by failing to maintain the privacy of the employees' information.

Pfizer recently obtained dismissal of the class action due to the class's failure to plead actual damages.[1] The court's focus on actual versus speculative damages demonstrates the importance of prompt notification. The more timely the notification, the less likely individuals will suffer actual damages (such as identity theft) and the more likely the company can avoid liability to an entire class.

While there is plenty of incentive to maintain an updated protocol to deal with data theft under the relevant legislation as it exists today, there are strong indications that those incentives are going to become even more compelling in the near future. Legislation is evolving in such a way that plaintiffs will be able to recover for harms that are not currently legally cognizable.

For example, while many states do not yet recognize the cost of credit monitoring in the wake of a data security breach to be a cognizable injury,[2] federal legislation that would explicitly do so was recently proposed. The stated goal of the Identity Theft Enforcement and Restitution Act of 2007 is to "enable increased federal prosecution of identity theft crimes and to allow for restitution to victims of identity theft." If this bill is passed, 18 U.S.C. § 3663(b) would be amended to force defendants convicted of identity-theft crimes to "pay an amount equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense."

Published in the February 2008 issue of Privacy & Data Security Law Journal.

The Identity Theft Enforcement and Restitution Act signals the increasing legal recognition of the damage incurred when a victim's personal information is wrongly accessed and a resolve to amend the laws to punish those in a position to prevent such wrongful access. In light of these expanding legal rights, companies that maintain large databases of personal identifying information ("PII") must have predetermined plans in place to deal with the likelihood of a security breach. Such plans allow companies to respond promptly and proportionately to data theft, minimizing the potential exposure to liability. Companies forced to analyze the issue for the first time in the hectic period after such a breach risk delays and errors that could easily translate to unnecessary civil liability.

CURRENT AND PROPOSED DATA-THEFT LEGISLATION

Identity theft (the use or the misuse of another individual's personal information without the individual's permission in order to commit fraud) results in billions of dollars in losses each year to individuals and businesses, according to a recent report by the President's Identity Theft Task Force. The prevalence and cost of identity theft to American consumers and companies has resulted in recent legislation that attempts to detect and prevent, and mitigate the damages of, identity theft and fraud.

As of October 2007, each financial institution or creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, is required to develop and implement an Identity Theft Prevention Program ("Program") for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor to:

- Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the Program;
- Detect red flags that have been incorporated into the Program;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

- Ensure that the Program is updated periodically to reflect changes in risks from identity theft.

In addition, the final rules require those affected to:

- Develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card; and
- Develop policies and procedures to follow upon receipt of a notice of address discrepancy from a consumer reporting agency.

Also in October 2007, the U.S. Senate proposed legislation to build upon previous bills designed to protect victims of identity theft. The Identity Theft Enforcement and Restitution Act of 2007 would:

- Give victims of identity theft the means to seek restitution for the loss of their time and the money they had to spend in an effort to restore their credit and remedy the residual harms of identity theft.[3] Currently, there is no remedy under federal law that allows for compensation to victims of identity theft for the time and effort it takes them to restore their credit;
- Expand the jurisdiction of federal computer-fraud statutes to cover small businesses and corporations;
- Focus on whether the victim's computer is used in interstate or foreign commerce, allowing for the prosecution of cases in which both the identity thief's computer and the victim's computer are located in the same state. Currently, in order to prosecute criminals under the federal law, sensitive identity information must have been stolen through an interstate or foreign communication;[4]
- Prosecute as a felony damage to ten or more computers occurring as a result of the use of spyware or keyloggers; and
- Prosecute as a misdemeanor any loss occurring as a result of damage to a victim's computer of less than $5,000. Under current law, only damages to a computer totaling more than $5,000 are prosecuted.

Published in the February 2008 issue of Privacy & Data Security Law Journal.

STEPS A COMPANY CAN TAKE TO MITIGATE THE RISKS OF, OR DAMAGES CAUSED BY, A SECURITY BREACH

There will always be a risk that a hacker will work around a security system or that an identity thief working from within a company will steal company-held personal or financial information. In light of this, what steps can a company take to protect itself from hackers or other identity thieves?

- Implement an Identity Theft Prevention Program pursuant to FACTA;
- Establish and maintain a comprehensive information security program. Upgrade security systems rather than waiting for a security breach;
- Obtain audits by an independent third-party security professional on an annual basis. It is prudent to conduct an audit after any upgrade, change to the system, or change in retention, disposition, or privacy policy;
- Implement and abide by a privacy policy that will help mitigate real or potential damages caused by a security breach;
- Conduct background checks on employees who have access to personal identifying information;
- Implement procedures to provide consumer data only to legitimate businesses for lawful purposes;
- Do not cover up a security breach. Thirty-five states, including California, Illinois, and New York, have enacted legislation requiring companies and/or state agencies to disclose security breaches involving personal information. Inform authorities and clients/customers immediately for a minimal lag time between the breach and disclosure of the breach. Any delay in disclosure could be construed by potential plaintiffs as a cover-up or nondisclosure; and
- Inform all clients/customers of the potential breach; disclosure of a security breach must be over-inclusive. Avoid sending out a second notice at a later date because the initial notification of the breach was

Published in the February 2008 issue of Privacy & Data Security Law Journal.

limited to a specific group. The second group could incur additional damages as a result of a delayed notification.

NOTES

[1] *Ponder v. Pfizer, Inc.*, 522 F.Supp 2d. 793 (M.D. La. 2007).

[2] *See Pisciotta v. Old National Bancorp*, 499 F. 3d 629 (7th Cir. Aug. 23, 2007).

[3] 18 U.S.C. § 3663(b).

[4] 18 U.S.C. § 1030(a)(2)(c).

Published in the February 2008 issue of Privacy & Data Security Law Journal.