VEDDER PRICE®

Privacy Litigation Update

January 2008

Companies Must Prepare for Data Theft

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 website 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 21st.

Based on the security team's review, the breach was limited to names, addresses, phone numbers, and e-mail addresses. However, on August 21st, 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 website 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 August 22nd, 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 29th, 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.

The amount of time Pfizer waited to inform the class members of the unauthorized disclosure will be a crucial issue in that litigation. Indeed, the complaint alleges that Pfizer breached its "duty to timely inform the class members of the unauthorized disclosure of their private information so that the class members could take appropriate measures to avoid unauthorized use of their private information and monitor their credit reports for fraudulent charges." If Pfizer has an up-to-date protocol in place to deal with this kind of data theft, it may be able to limit any recovery stemming from the alleged breach of this duty.

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 (*see Pisciotta v. Old National Bancorp*, No. 06-3817, 2007 U.S. App. LEXIS 20068 (7th Cir. Aug. 23, 2007)), 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."

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[1] 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 United States 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. 18 U.S.C. § 3663(b). 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

[1] Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), the Identity Theft Prevention Program, enacted 10/31/07, and the proposed Identity Theft Enforcement and Restitution Act of 2007.

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. 18 U.S.C. § 1030(a)(2)(c);

- 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.

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

[2] Cal. Civ. Code § 1798.82, 815 Ill. Comp. Stat. 530/1 et seq., N.Y. Bus. Law § 899-aa.

Vedder Price's privacy litigation team has represented Fortune 500 and other companies in mitigating the risks associated with data theft, complying with PCI standards and the FACTA Disposal Rule, and litigation involving loss and/or wrongful use of consumer data. For further information on Vedder Price's privacy litigation team, please contact Timothy J. Carroll at 312-609-7709 or tcarroll@vedderprice.com, Bruce A. Radke at 312-609-7689 or bradke@vedderprice.com, or Michael J. Waters at 312-609-7726 or mwaters@vedderprice.com.

VEDDER PRICE P.C.

About Vedder Price

Vedder Price P.C. is a national, full-service law firm with over 250 attorneys in Chicago, New York, Washington, D.C. and New Jersey.

Commercial Litigation Group

The Vedder Price litigation practice group gives constant attention to providing cost-effective and efficient legal services, regardless of the size of the matter, and continuously updates clients with respect to estimated and actual expenses of litigation. Over the years, Vedder Price trial attorneys have been involved in a significant number of cases that have shaped the course of the law in various substantive areas at the local, state and national level. In addition to general business litigation experience, Vedder Price litigators have special knowledge in a number of areas, including the following:

- Antitrust, Unfair Competition and Intellectual Property Litigation
- Bankruptcy and Creditor Rights Litigation
- Commercial and Financial Institution Litigation
- Consumer Litigation
- Gaming Law
- Insurance Litigation
- Manufacturers Liability
- Privacy Litigation
- Real Estate and Land Use Disputes
- Records Management and eDiscovery
- Securities Litigation
- Tax Litigation

Privacy Litigation Update is published periodically by the law firm of Vedder Price P.C. It is intended to keep our clients and interested parties generally informed about privacy-consumer issues. It is not a substitute for professional advice. For purposes of the New York State Bar Rules, this bulletin may be considered ATTORNEY ADVERTISING. Prior results do not guarantee a similar outcome.

Contact the following for privacy-related counseling and risk-mitigation efforts:

Timothy J. Carroll
312-609-7709

John H. Eickemeyer
212-407-7760

Amy E. Hallbrook
312-609-7757

Diane M. Kehl
312-609-7664

James S. Montana
312-609-7820

Michael R. Mulcahy
312-609-7513

Bruce A. Radke
312-609-7689

Michael J. Waters
312-609-7726