PROTECTING YOUR DATA PROTECTS THE BOTTOM LINE

by
Shawn J. Organ
and
Jonathan K. Stock

In 2003, the California law requiring the reporting of data security breaches went into effect, and over the next four years, more than 300 million records were lost or stolen; 34 million were expected to be stolen in 2008.[1] Protecting data privacy has evolved into one of the biggest challenges, financial expenditures, and possible sources of legal exposure for companies operating in this new digital world. Companies routinely keep and store data about their customers. Often this information includes sensitive details that customers want and expect the company to safeguard and keep private. Chances are that your credit card information, medical records, Social Security number, and bank account numbers are already in the possession of several hundred companies, government agencies, and nonprofit organizations.

In the right hands, this personal information is a resource that enables efficient and effortless transactions and permits companies and government agencies to provide desired products and services. The same information, however, can spell personal and financial disaster in the wrong hands. Identity theft has claimed an ever-growing list of victims and by one estimate has now struck one in five Americans.[2] The Federal Trade Commission ("FTC") estimates that each year as many as 9 million Americans become identity-theft victims.[3] A survey conducted by the FTC showed that identity-theft losses to businesses and financial institutions totaled nearly $48 billion in a single year.[4] Security breaches at companies that store personal data have contributed to the growth of identity theft.

THEFT AND CONSEQUENCES

Several of these security breaches in recent years have made headlines, perhaps none more so than the massive security breach involving T.J. Maxx. The incident involving T.J. Maxx has been described as the largest data breach in U.S. corporate history.[5] The total cost of the T.J. Maxx security breach has been staggering: The TJX Companies, the parent company of T.J. Maxx, told *The Boston Globe* that "its costs from the largest computer data breach in corporate history, in which thieves stole more than 45 million customer credit and debit card numbers, have ballooned to $256 million."[6] Those costs stem from, among other things, repairing the company's computer system, conducting investigations, and defending the lawsuits and other claims arising from the theft. However, "[s]everal analysts have estimated TJX's costs could run as high as $1 billion, including legal settlements and lost sales."[7]

While it is often difficult to catch the perpetrators of identity theft, the Justice Department recently announced the indictment of 11 individuals in connection with the T.J. Maxx data security breach.[8] According to the indictment, the thieves gained access to the credit and debit card data of millions of customers in part by simply driving around in a car with a laptop computer, looking for accessible wireless networks, and then installing special software that captured the credit and debit card information from the unsecured networks.[9]

A web site that tracks data privacy breaches lists hundreds of data security breaches that have occurred in the United States since 2005.[10] While not every security breach results in identity theft, the exposure of personal information and the risk of identity theft have forced businesses and consumers alike to commit substantial time and resources. Businesses are constantly updating their technology in a race with identity thieves, and they incur substantial costs if personal data in their possession is ever exposed. Consumers have taken time-consuming and burdensome steps to shield their identities and financial resources from identity theft or, even worse, to remedy the harm caused by identity theft.

With the threat of identity theft on the rise, state governments have taken an active role in regulating the steps a company must take after a security breach. At least 44 states, as well as the District of Columbia and Puerto Rico, have enacted legislation requiring notification for security breaches involving personal information.[11] Typically, these laws require a company whose data has been breached to notify the persons whose identity and personal information have been put at risk. While the laws requiring notification give consumers a chance to quickly take steps to re-shield their identity (*i.e.*, cancel credit cards, review credit reports, place a credit hold, etc.), they have done little or nothing to stop the spread of identity theft.[12]

Threats to data privacy have also inspired a response from the federal government. Most notably, the Federal Trade Commission has promulgated rules to govern data privacy in the financial and consumer credit industries.[13] Also, to implement the Fair and Accurate Credit Transactions Act ("FACTA"), the FTC and the federal banking agencies have jointly issued new rules for financial institutions and creditors governing identity theft.[14]

Now the threat of litigation is making data security breaches even more costly and adding extra incentives for businesses to secure their data. Plaintiffs have begun filing suit against companies that suffer data breaches. The T.J. Maxx data breach, for example, spawned at least a half-dozen class actions. As one commentator noted, what makes the T.J. Maxx case so compelling for class actions is that: (1) "unlike the majority of reported security breaches, the TJX intrusion has been demonstratively linked to subsequent fraudulent transactions"; and (2) "early media reports implied that the company was negligent in safeguarding its data," including the suggested absence of a firewall.[15]

Class actions were also filed this year against the Hannaford Bros. supermarket chain for a data breach involving customer credit card numbers. Hannaford had previously notified its customers that a breach of its computer system between December 2007 and March 2008 potentially exposed 4.2 million credit and debit card numbers and resulted in 1,800 fraud cases to date.[16] Only a couple days after the announcement, Hannaford was sued.[17] These suits allege, among other things, that Hannaford was negligent in protecting customer data and failing to promptly disclose the breach of that data to the public.[18]

TD Ameritrade also became the target of a class action after hackers in late 2007 stole the identities of at least 6.3 million TD Ameritrade customers. The parties attempted to settle the suit when they reached agreement for TD Ameritrade to provide spam-blocking software to the class and $1.87 million in fees to the plaintiffs' attorneys,[19] but the judge overseeing the case rejected the proposed settlement as potentially unfair to the class.[20]

Not every data security breach starts with a thief. Unlike the T.J. Maxx and TD Ameritrade cases, where an organized group successfully pirated company data, many data security breaches have more mundane origins. In the summer of 2008, a number of customers with Wagner Resource Group, among them Supreme Court Justice Stephen Breyer, had their personal data exposed, including names, birth dates, and Social Security numbers. The exposure took place when an employee of Wagner Resource Group accessed a file-sharing network called LimeWire.[21] When the employee tried to "trade some music, or maybe a movie," he "inadvertently opened the private files of his firm."[22]

In another example of inadvertent data exposure, two banks recently made news after an unencrypted backup tape full of personal data was lost in transit on February 23, 2008. After the data of approximately 4.5 million people went missing, it did not take long for the first lawsuit to be filed. A group of bank customers filed a civil suit in Bridgeport, Connecticut, seeking class action status and charging those banks with negligence, invasion of privacy, and breach of fiduciary duty.[23] The exposure of personal data, regardless of its source, presents a tempting target for identity thieves and has the potential to embroil a company in litigation.

The cases filed against companies that suffered data security breaches have yielded mixed results, with a number of companies reaching settlements and others successfully defending. TJX, whose data security breach made major headlines, reportedly settled a number of the lawsuits filed against it, including one for an amount in excess of $40 million.[24]

However, not every data security breach leads to liability. Instead, case law has held that identity exposure alone, absent evidence of actual identity theft caused by that exposure, is insufficient to support a claim for damages. Such cases include, for example, *Pisciotta v. Old National Bancorp*; *Kahle v. Litton Loan Serv. LP*; *Randolph v. ING Life Ins. and Annuity Co.*; *Giordano v. Wachovia Sec., LLC*; *Forbes v. Wells Fargo Bank, N.A.*; *Guin v. Brazos Higher Educ. Serv. Corp.*; *Hendricks v. DSW Shoe Warehouse*; and *Stollenwerk v. Tri-West Healthcare Alliance*.[25] While most cases frame the absence of damages as a failure to prove all the elements of a claim, in some instances, the cases hold that the federal courts lack jurisdiction because plaintiffs whose data has been compromised but not yet misused have not suffered an injury-in-fact necessary for Article III standing.[26] Several common factual threads unite these cases. In almost every instance, the typical plaintiff has not suffered from identity theft. Instead, the plaintiff is alleged to have incurred costs from the increased risk of identity theft. Those costs include the time and expense necessary to purchase credit card monitoring and protection services. Almost invariably, the cases are centered around a claim for common-law negligence and rely upon the argument that the defendant failed to meet its duty of care to safeguard and protect the plaintiff's data.

The courts in the above cases have rejected these negligence-based claims and have not held the companies liable for the mere exposure of data. The central fault of these causes of action is that the plaintiff, who has not suffered from identity theft, cannot prove actual damages.[27]

The courts, in addition to noting the absence of actual damages, have often found support for rejecting liability from diverse sources. First, some courts have looked to the analogous field of toxic tort litigation to explain why the speculative injury of a future identity theft is not compensable.[28] Some courts also point to the absence of any private right of action for a data breach in state law to support the noncompensable nature of the claim.[29]

Finally, in *Guin*,[30] the court noted in exculpatory fashion that the defendant, despite the data breach, had demonstrated good data protection practices, commenting that the defendant "had policies in place to protect the personal information, trained [its employee] concerning those policies, and transmitted and used data in accordance with those policies."

Several broad lessons can be gleaned from the divergent outcomes of cases where some companies have been forced into settlement while others have defended successfully. First, the exposure of data alone does not necessarily lead to liability. The cases demonstrate that the occurrence of identity theft poses a much greater risk to companies than the mere exposure of data. The degree of that risk can be mitigated by a company that adopts and diligently follows the best policies and practices to safeguard its data. It is no coincidence that companies like T.J. Maxx have paid significant sums to settle cases that have alleged lax data protection practices resulting in identity theft. In the event of a data security breach, time is of the essence. By promptly seeking counsel and complying with all applicable laws (including the many state notification statutes), a company can reduce its risks and limit the likelihood that any data breach can be successfully exploited.

PRACTICAL STEPS AND SOLUTIONS

The Federal Trade Commission has put together a list of five steps that businesses can take to minimize their exposure to data theft.[31] These are relatively simple steps that may seem intuitive but are all too often overlooked.

First, every business that stores personal data should take stock of what data exists and where it is kept. Businesses should: (1) take inventory of all computers, laptops, flash drives, and other storage equipment to find out where data is kept throughout the company; (2) track the personal information used and relied upon by each department; and (3) pay special attention to the types of personal information commonly sought by identity thieves, such as Social Security numbers and credit card information.

Second, keeping personal data on file carries a risk. Businesses should therefore scale down their storage of any information that does not support legitimate business needs.

Third, businesses must safeguard the information they keep. Personal data should not be something that is open to everyone in the company. Employee access should be a matter of business necessity, and any unauthorized access from within

continued on page 40

continued from page 27

or outside the company should be blocked. For physical documents, this can be a matter of keeping them under lock and key. For electronic data, businesses have a number of important tools that they should put to good use: firewalls, password protection, and up-to-date anti-virus and anti-spyware programs are a must. Businesses that transmit personal data over a wireless network or store data on a computer with internet access should recognize the threat posed by hackers and take steps to secure their networks.

Fourth, when a business no longer needs the personal data that it keeps on file, that data should be destroyed consistent with the company's document-retention policy. Old credit card numbers and outdated customer records pose an attractive target to identity thieves. Oftentimes this older data is not as well secured by the company keeping it. Paper or other physical records can be shredded, burned, or pulverized. Electronic records can be overwritten or wiped clean through available software solutions.

Fifth, any business that stores personal data must have a plan to respond to data security threats. That plan should include steps for stopping, investigating, and reporting any attempted or successful data security breach. Once a breach has occurred, the business should promptly seek counsel and take steps to remedy the breach. Those steps can include: (1) curing the source of the data breach; (2) identifying what, if any, data was compromised; and (3) complying with all applicable customer-notification laws. A fast response to a data breach makes it more difficult for identity thieves to successfully use any information they might obtain.

While this may seem like easy advice to follow, far too many businesses have no plan in place or refuse to seek advice following a data breach. In a survey of business executives and IT security officers in U.S. companies conducted by the Ponemon Institute, only 43 percent of respondents said their companies had incident response plans in place for data security breaches, and 82 percent failed to consult with legal counsel before responding to an incident.[32]

In many ways, companies that store personal data are in a never-ending race with identity thieves. As companies come up with better ways to safeguard information, identity thieves find more clever ways to obtain it. A company that follows the best practices to safeguard its data is ultimately safeguarding its bottom line. In 2007, the estimated cost of a data security breach amounted to $197 per compromised record and $6.3 million per incident.[33] By taking steps now to safeguard personal data, a company can also safeguard its financial future. ■

SHAWN J. ORGAN
1.614.281.3961
sjorgan@jonesday.com

JONATHAN K. STOCK
1.614.281.3967
jkstock@jonesday.com

[1] http://www.etiolated.org/statistics (web sites last visited Feb. 6, 2009).

[2] "Survey: One in Five Americans Have Been Victims of Identity Fraud," *Insurance Journal*, July 8, 2005, http://www.insurancejournal.com/news/national/2005/07/08/57054.htm.

[3] http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[4] "FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers," Sept. 3, 2003, http://www.ftc.gov/opa/2003/09/idtheft.shtm.

[5] "TJX consumer data theft largest in history," Jacqui Cheng, Ars Technica, Mar. 30, 2007, http://arstechnica.com/news.ars/post/20070330-tjx-consumer-data-theft-largest-in-history.html.

[6] "Cost of data breach at TJX soars to $256m," Ross Kerber, *The Boston Globe*, Aug. 15, 2007, http://www.boston.com/business/globe/articles/2007/08/15/cost__of__data__breach__at__tjx__soars__to__256m/?page=2.

[7] *Id.*

[8] "11 charged in largest I.D. theft in U.S. history," Andrea Chang and Joseph Menn, *Los Angeles Times*, Aug. 6, 2008.

[9] *Id.*

[10] http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP.

[11] List compiled by the National Conference of State Legislatures as of Sept. 16, 2008; http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

[12] "Do Data Breach Disclosure Laws Reduce Identity Theft?" Sasha Romanosky, Rahul Telang, and Alessandro Acquisti from Carnegie Mellon University (June 2008) ("We find no statistically significant effect that laws reduce identity theft, even after considering income, urbanization, strictness of law and interstate commerce."), http://weis2008.econinfosec.org/papers/Romanosky.pdf.

[13] *See*, *e.g.*, 16 CFR Parts 313 and 314 (establishing privacy and security rules for financial institutions adopted under the Gramm-Leach-Bliley Act, which require financial institutions to: (i) give consumers notice of their data privacy policies; (ii) limit their use of consumer data; and (iii) adopt security plans to protect data confidentiality); 16 CFR Part 682 (requiring the proper disposal of consumer data from financial statements and credit reports).

[14] 15 U.S.C. §1581m(e).

[15] "TJX Being Sued Over ID Thefts," PatriotLedger.com, Feb. 17, 2007, http://identitytheft911.org/alerts/alert.ext?sp=870.

[16] "Grocer Hannaford hit by computer breach," Ross Kerber, *The Boston Globe*, Mar. 18, 2008, http://www.boston.com/business/articles/2008/03/18/grocer__hannaford__hit__by__computer__breach/.

[17] "Hannaford hit by class-action lawsuits in wake of data-breach disclosure," Jaikumar Vijayan, *Computerworld*, Mar. 20, 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9070281.

[18] *Id.*

[19] *See Elvey v. TD Ameritrade*, Case No. C 07 2852 VRW (U.S.D.C. for the N.D. Cal.), Class Action Settlement Agreement, filed May 30, 2008, http://blog.wired.com/27bstroke6/files/ameritrade.pdf.

[20] *See* "Judge Scuttles Ameritrade Hacking Settlement," David Kravets, *Wired*, June 13, 2008, http://blog.wired.com/27bstroke6/2008/06/judge-scuttles.html.

[21] "Justice Breyer Is Among Victims in Data Breach Caused by File Sharing," Brian Krebs, WashingtonPost.com, July 9, 2008, http://washingtonpost.com/wp-dyn/content/article/2008/07/08/AR2008070802997__pf.html.

[22] *Id.*

[23] "The Data Breach," HartfordBusiness.com, June 9, 2008, http://www.hartfordbusiness.com/news5711.html.

[24] *See* "TJX, Visa reach $40.9M settlement for data breach," Mark Jewell, *USA Today*, Nov. 30, 2007, http://www.usatoday.com/money/industries/retail/2007-11-30-tjx-visa-breach-settlement__N.htm.

[25] *Pisciotta v. Old National Bancorp*, 499 F.3d 629, 639–640 (7th Cir. 2007) (cost of credit card monitoring not recoverable as compensable damages); *Kahle v. Litton Loan Serv. LP*, 486 F. Supp. 2d 705, 712 (S.D. Ohio 2007); *Randolph v. ING Life Ins. and Annuity Co.*, 486 F. Supp. 2d 1 (D.D.C. 2007); *Giordano v. Wachovia Sec., LLC*, 2006 U.S. Dist. LEXIS 52266, at *12 (D.N.J. July 31, 2006); *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006); *Guin v. Brazos Higher Educ. Serv. Corp.*, 2006 U.S. Dist. LEXIS 4846, at *15 (D. Minn. Feb. 7, 2006); *Hendricks v. DSW Shoe Warehouse*, 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006); *Stollenwerk v. Tri-West Healthcare Alliance*, 2005 U.S. Dist. LEXIS 41054, at *10 (D. Ariz. Sept. 8, 2005).

[26] *See Randolph*, 486 F. Supp. 2d at 7–8; *Giordano*, 2006 U.S. Dist. LEXIS 52266 at *12.

[27] *Pisciotta*, 499 F.3d at 639 ("Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."); *Forbes*, 420 F. Supp. 2d at 1021 (noting plaintiffs' "expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized").

[28] *Pisciotta*, 499 F.3d at 638–639 (noting that the recovery of damages for toxic tort liability "requires more than an exposure to a future potential harm"); *Stollenwerk*, 2005 U.S. Dist. LEXIS 41054, at **10–11.

[29] *Pisciotta*, 499 F.3d at 637 (upholding trial court's award of summary judgment, while noting that "[h]ad the Indiana legislature intended that a cause of action should be available against a database owner for failing to protect adequately personal information, we believe that it would have made some more definite statement of that intent"); *Hendricks*, 444 F. Supp. 2d at 783 (noting in favor of dismissal that "[t]here is no existing Michigan statutory or case law authority to support plaintiff's position that the purchase of credit card monitoring constitutes either actual damages or a cognizable loss").

[30] 2006 U.S. Dist. LEXIS 4846, at *15 (D. Minn. Feb. 7, 2006).

[31] *See* "Protecting Personal Information: A Guide for Business," Federal Trade Commission, http://www.ftc.gov/infosecurity/.

[32] *See* "Survey: Companies disregard data security breach risks," Robert Westervelt, SearchSecurity.com, May 17, 2007, http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185__gci1294452,00.html#.

[33] *See* "Press Release: Ponemon Study Shows Data Breach Costs Continue to Rise," PGP, Nov. 28, 2007, http://www.pgp.com/newsroom/mediareleases/ponemon-us.html.