

INVESTIGATIONS & COMPUTER FORENSICS

ALM

Web address: <http://www.nylj.com>

MONDAY, MAY 12, 2008

Data Breaches: Expect A Rise in **Litigation**

Spike in loss of electronic data makes companies vulnerable to lawsuits.

**BY JIM WALDEN,
ALEXANDER H. SOUTHWELL
AND AARON GOODMAN**

OVER the last several years, corporate data breaches have been regularly splashed across the front pages of the nation's newspapers, causing nightmares for corporate executives. Ever-increasing digitization in areas such as business, bank-

Jim Walden, the former chief of the computer crimes and intellectual property section of the Brooklyn U.S. Attorney's Office, is a partner at Gibson, Dunn & Crutcher and the co-chair of its white collar defense and investigations group. **Alexander H. Southwell** is of counsel at the firm, an adjunct professor of law at Fordham University School of Law and a former federal prosecutor in the Southern District of New York. **Aaron Goodman** is an associate at the firm.

ing and accounting has led multinationals to collect and retain inestimable quantities of personal information about employees, customers and counter-parties.¹ The negligent (or even innocent) loss of electronic data to cybercriminals inflicts billions of dollars of damage on our economy, as personal information has become a sought-after treasure trove for cyber-criminals.² In fact, recent reports note that the number of attacks on credit and debit card processing systems has more than doubled from 2006 to 2007, and that trend appears to be continuing into 2008.³

These costs are likely to escalate as, in an increasing trend, corporations are also being pummeled with civil litigation related to data breaches. The recently announced data breach at grocer Hannaford Brothers Co. illustrates the trend. On March 17, 2008, Hannaford announced that cyberbandits had breached its system, obtaining access to personal-financial information of nearly 4.2 million customers.⁴ Just three days after the announcement, plaintiffs' lawyers filed four class actions against Hannaford. Since then, lawyers have filed an additional 12 complaints, requiring Hannaford to defend litigation from Florida to Maine.⁵

Hannaford is not alone: TJX, a retailer that operates T.J. Maxx and Marshall's stores, faced a federal investigation and an onslaught

of follow-on civil litigation⁶ after announcing a breach widely reported as the largest data-security breach in U.S. history where computer "hackers" stole at least 45.7 million credit and debit records.⁷

Although data breaches can occur in a wide variety of ways—from lost or stolen employee laptops to hacked computer networks—most companies face a similar array of implications following discovery of a breach. As an initial and immediate matter, a thorough forensic investigation is critical to ascertain the scope and nature of the data breach. Only a complete assessment of the digital evidence will help to determine how the breach occurred, how recurrences can be prevented, and precisely what data—and in what form—was compromised, all of which will contribute to ascertaining the best course of action.

State Laws

Forensic investigations are also critical to guide a corporation through the maze of state data breach notification laws. Such laws will require varying levels of compliance, depending on the nature of the breach and of the entity's operations. California's data breach law, which has served as a model for many other states, demands that upon discovering a breach of personal

information, a business “shall disclose any breach of the security of the system” to any affected persons “in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.”⁸

While not required in California, some states also require notifying consumer reporting agencies.⁹ Thus, compliance with state law often forces a company to go public by announcing the security breach, thereby beginning the public relations nightmare. After the breach at TJX, for example, the company sent letters to the estimated 455,000 customers whose information had been compromised and offered them credit monitoring, helping make the data breach a front-page story.¹⁰ Beyond the bad publicity, only mere months after the breach, TJX had already incurred \$5 million for the investigation and for new computer security.¹¹

Regulatory Scrutiny

In addition to the media scrutiny focused on corporate data breaches, companies suffering data breaches have increasingly been subjected to regulatory scrutiny, typically spearheaded by the Federal Trade Commission and state Attorneys General. Indeed, in 2006, the FTC established its Division of Privacy and Identity Protection, specifically tasked to investigate data breaches. As of March 2008, the FTC has brought 20 cases against businesses for failing to maintain reasonable security in protecting “sensitive consumer information” and investigated many others.¹²

FTC actions are routinely resolved through settlements, which may include hefty fines and often require the implementation of comprehensive information security plans with regular independent audits. In January 2006, the FTC announced a record settlement with ChoicePoint Inc., which had disclosed the year before that the personal-financial information of 163,000 consumers had been compromised. The settlement required ChoicePoint to pay \$10 million in civil penalties (the largest civil penalty in FTC history), to provide \$5 million for consumer redress and to establish and

maintain a comprehensive information security program including administrative, technical and physical safeguards, as well as audits by an independent third-party security professional every other year for 20 years.¹³ The FTC’s June 2005 settlement with BJ’s Wholesale Club, which had been charged with failing to take appropriate security measures to protect the sensitive information of thousands of its customers, also required implementing a new information security program and biennial audits for 20 years,¹⁴ as did the FTC’s September 2007 settlement with TJX.¹⁵

Litigation

As stated, corporations suffering data breaches are also routinely contending with follow-on civil suits—private, often class, actions, seeking damages for the potential economic losses and emotional distress allegedly caused by the potential misuse of the disclosed personal information. Increasingly, these suits are filed soon after the data breach is publicly announced—much like “stock drop” securities class actions—thereby adding negative publicity and causing further distractions. Indeed, the first four lawsuits against Hannaford were filed just three days after the company announced that there had been a security breach.

Data breach litigation typically alleges causes of action grounded in tort and contract: negligence, breaches of fiduciary duty, breaches of real and implied contracts, invasion of privacy and emotional distress. Some causes of action are grounded in state law, such as consumer protection acts, unfair trade practices acts and state data breach notification laws. Plaintiffs in these lawsuits seek damages arising from the fear of potential identity theft, including fraudulent charges to their accounts, credit monitoring costs, identity theft insurance costs, credit report costs, emotional distress from fear of fraud, damage to credit history and loss of privacy. Courts have been hesitant to permit suits for such speculative damages, thus dismissing suits where plaintiffs had not yet been victims of any identity fraud.

In the recent case of *Randolph v. ING Life Insurance & Annuity Co.*, plaintiffs brought a consumer class action in District of Columbia federal court for invasion of privacy, gross negligence and negligence against ING following an announcement of the theft of an employee laptop from that employee’s home containing the personal information of 13,000 government workers and retirees.¹⁶ Plaintiffs argued, inter alia, that the theft exposed them to “substantial risk of identity theft,” and that as a “direct and proximate result,” they “have been exposed to a risk of substantial harm and inconvenience, and have incurred or will incur actual damages in purchasing comprehensive credit reports and/or monitoring of their identity and credit for the definite future.”¹⁷ However, none of the plaintiffs asserted that they had actually been the victim of any identity theft.¹⁸

As stated briefly above, litigation of this type does not generally progress beyond the pleadings stage due to an absence of actual damages. As an illustration, in *Randolph*, ING succeeded on a motion to dismiss, arguing that plaintiffs lacked standing to sue because they proved no actual damages and, thus, no “recognized injury.”¹⁹ The court agreed, citing a long line of “lost data” cases in which courts held that “an allegation of increased risk of identity theft due to lost or stolen personal data, without more, is insufficient to demonstrate a cognizable injury.”²⁰ Thus, plaintiffs failed to demonstrate the “injury in fact” necessary for the constitutional requirement of Article III standing.²¹ Moreover, the court also recognized that credit monitoring services, even if the plaintiffs were to have actually alleged payment for such services, cannot constitute actual injury.²²

Guin v. Brazos Higher Education Service Corporation Inc. had a similar result.²³ There, plaintiff brought a negligence suit against Brazos after it announced the theft of a laptop containing personal information for 550,000 customers. Granting summary judgment in favor of Brazos, the court held that Brazos had no duty of protection (under the Gramm-Leach-Bliley Act),²⁴ that Brazos acted with reasonable

care in handling the information and that Brazos's inability to foresee and deter the specific theft was not a breach of a duty of reasonable care.²⁵ Because neither of plaintiff's identity nor personal information was used in any fraud, the court also ruled that the absence of damages was likewise fatal to plaintiff's claim.²⁶ Consequently, the court dismissed the case with prejudice.

Using similar reasoning, the U.S. Court of Appeals for the Seventh Circuit recently dispatched another action for damages arising from a data breach.²⁷ In *Pisciotta v. Bancorp*, the court held that speculative damages for fraud and for credit monitoring fees were not supported by state law—"[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."²⁸ Importantly, the court also held that Indiana's state data breach notification law would not serve to permit such allegations of damage as that statute only creates a duty to disclose and places enforcement in the hands of the Attorney General; it creates no private right of action.²⁹

Plaintiffs have not been sheepish in the face of these dismissals. For example, in the Hannaford cases, plaintiffs raised claims of common law negligence, breach of contract (real and implied) and breach of fiduciary duty.³⁰ The cases seek damages including out-of-pocket losses due to fraud, the costs of credit monitoring, the cost of identity theft insurance, the cost of credit reports, emotional distress damages arising from fear and apprehension of fraud and identity theft, loss of privacy, anxiety and loss of control of personal information.³¹ Several of the cases sought damages under Maine's Unfair Trade Practices Act.³²

While it is too soon to accurately predict the litigation landscape, the trend seems to be grounding more lawsuits in state law statutes, and for common law allegations, alleging more specific and provable damages. The better plaintiffs get on the damages front, the farther along the cases will be able to move. This could mean the potential for more costly discovery before a suit is resolved or settled. While the hurdles for plaintiffs remain high,

these lawsuits have become a fact of life in today's litigious society. Corporations suffering data breaches thus must now routinely face an onslaught of civil litigation in addition to the negative publicity and regulatory scrutiny coming from data breaches and their announcements. Given the increasing digitization of the economy and society, companies should brace for these lawsuits when the almost inevitable data breach occurs.



1. "Personal Information" is a term of art used in state data breach notification laws, generally defined as an individual's first name or first initial and last name, in combination with that individual's social security number, driver's license number or credit, debit or account number (in combination with a required access code). See, e.g., N.Y. GEN. BUS. LAW §899aa(b) (2007). Two states also include medical information. See, e.g., ARK. CODE ANN. §4-110-103(7) (2007); CAL. CIVIL CODE §1798.82(e) (2007).

2. Andrew K. Burger, "The Costs of ID Theft, Part 2: Fixing the System," E-Commerce Times, Feb. 6, 2008, available at www.ecommercetimes.com/story/61542.html.

3. "Data Breaches: Attacks Seeking Credit Card Data Double, PCT DSS Efforts Crucial, Visa Official Says," 7 Privacy & Security Law 13 (March 31, 2008).

4. "Data Breaches; Hannaford Faces a Dozen More Class Actions Over Breach of Customer Payment Card Data," 7 Privacy and Security Law 14 (April 7, 2008).

5. Id.

6. "First TJX Class Actions Brought in U.S., Canada," 10 Consumer Financial Services Law Report, Data Security 16 (Feb. 21, 2007).

7. Jenn Abelson, "Breach of data at TJX is called the biggest ever," Boston Globe, March 29, 2007.

8. CAL. CIVIL CODE §1798.82 (a). Most states adopt this language, with only minor variations. See, e.g., MD. CODE ANN. §14-3504(b)(3) (2007) ("as soon as reasonably practicable"); OHIO REV. CODE ANN. 1349.19(B)(2) (2007) ("in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach").

9. See, e.g., COL. REV. STAT. §6-1-716(2)(d) (2007); FLA. STAT. §817.5681(12) (2007); GA. CODE ANN. §10-1-912(d) (2007); INDIANA CODE §4-1-11 (2007).

10. Abelson, supra note 7.

11. Id.

12. "Data Breach: FTC Settlements Require Data Brokers, Retailer to Secure Customer Information," 7 Privacy & Security Law 13 (March 31, 2008).

13. Press Release, Federal Trade Commission, "ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress" (Jan. 26, 2006), available at <http://www.ftv.gov/opa/2006/01/choicepoint.htm>.

14. Press Release, Federal Trade Commission, "BJ's Wholesale Club Settles FTC Charges" (June 16, 2005), available at <http://www.ftc.gov/opa/2005/06/bjswholesale.shtm>.

15. Press Release, Federal Trade Commission, "Agency Announces Settlement of Separate Actions Against Retailer TJX" (March 27, 2008), available at

<http://www.ftc.gov/opa/2008/03/datasetec.shtm>. TJX separately settled lawsuits brought by card-issuing banks for around \$66 million, and a consumer class action for a variety of vouchers, cash benefits and reimbursements, credit monitoring and identity theft insurance, and up to \$6.5 million for attorney fees. Other litigation and governmental investigations related to TJX are ongoing.

16. 486 F.Supp.2d 1 (D. D.C. 2007).

17. Id. at 4.

18. Id.

19. Id. at 6.

20. Id.

21. Id. at 6-7; *Bell v. Axiom Corp.*, No. 4:06CV00485, 2006 U.S. Dist. LEXIS 72477 (E.D. Ark. Oct. 3, 2006) (dismissing action as a matter of law for lack of standing where "Plaintiff has not alleged that she has suffered anything greater than an increased risk of identity theft"); *Giordano v. Wachovia Sec., LLC*, No. 06-476, 2006 U.S. Dist. LEXIS 52266 at *12 (D. N.J. July 31, 2006) ("Plaintiff's claims, at best, are speculative and hypothetical future injuries. A complaint alleging the mere potential for an injury does not satisfy Plaintiff's burden to prove standing."); *Hendricks v. DSW Shoe Warehouse Inc.*, 444 F.Supp.2d 775 (W.D. Mich. 2006), (dismissing breach of contract claim arising from data theft as a matter of law for failure to allege any actual damages).

22. *Randolph*, 484 F.Supp.2d at 19-20 ("expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized").

23. *Guin v. Brazos Higher Ed. Serv. Comp. Inc.*, No. 05-668, 2006 U.S. Dist. LEXIS 4846 (D. Miss. Feb. 7, 2006).

24. Id., at *8-9; see 15 USC §6801 (act created to protect against unauthorized access to or use of records which could result in substantial harm or inconvenience to any customer of a financial institution).

25. Id. at *12.

26. Id. at *16.

27. *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007).

28. Id.

29. Id.

30. See, e.g., *Nenni v. Hannaford Bros., Co.*, No. 1:08-cv-106-JL (D. N.H. March 20, 2008); *Doherty v. Hannaford Bros., Co.*, No. 2:08-cv-00089-DH (D. Ma. March 19, 2008); *Wheeler v. Hannaford Bros., Co.*, No. 2:08-cv-00091-DBH (D. Ma. March 20, 2008); *Ryan v. Delhaize America Inc.*, No. 1:08-cv-00086-JAW (D. Ma. March 18, 2008); *Bradbury v. Delhaize America Inc.*, No. 2:08-cv-00093-DBH (D. Ma. March 20, 2008).

31. Id.

32. See *Ryan*, No. 1:08-cv-00086-JAW; *Bradbury*, No. 2:08-cv-00093-DBH.