

Commentary

Potential Business Liability For Failure To Secure Consumer Data

By
Randy Gainer

[Editor's Note: Randy Gainer is a partner in the Seattle office of Davis Wright Tremaine LLP. His practice emphasizes litigating computer system disputes and advising businesses about data security issues. See <http://www.dwt.com/lawdir/attorneys/GainerRandy.cfm>. The views expressed in this article are those of the author and not of Davis Wright Tremaine, any client of the firm or Mealey Publications. Copyright 2005 by the author. Responses are welcome.]

I. BJ's Wholesale Club — Poster Child For Data Theft

For more than a month in early 2005, data thieves monitored unencrypted data transmitted over WiFi systems of retail stores in an area just south of downtown Miami. A BJ's Wholesale Club outlet was among the stores the thieves monitored. The thieves used BJ's WiFi signal to gain access to the store's on-site computers. Eric Dash, *Main Street in the Crosshairs*, N.Y. TIMES, July 26, 2005, at C1, available at <http://www.nytimes.com/2005/07/26/business/26card.html>. BJ's used the WiFi system only to connect its on-site computers with inventory scanning devices in the store, but once the thieves gained access to BJ's computers, they used default user IDs and passwords to download bank card data. Charles H. Kennedy and Christina A. K. Hickerson, *The BJ's Case: Data Insecurity Meets the FTC's "Unfairness" Doctrine*, 4 Privacy & Security Law Report (BNA) 946 (July 18, 2005). The thieves made fraudulent purchases with BJ's customers' credit and debit cards. Many customers could not use their accounts until new cards were issued. *Id.*, 946-47.

The Federal Trade Commission issued a complaint against BJ's for failing to provide "reasonable security" for its computer network. The FTC alleged that BJ's failed to encrypt consumer information when BJ's transmitted or stored data at BJ's locations; created unnecessary risks for the information by storing data for up to 30 days, which violated bank security rules; failed to change commonly-known default user IDs and passwords; failed to use available WiFi security measures; and failed to use measures to detect unauthorized access to BJ's computer networks or to conduct security investigations. Press Release, BJ's Wholesale Club Settles FTC Charges, <http://www.ftc.gov/opa/2005/06/bjswholesale.htm>.

To settle the FTC's complaint, BJ's agreed, among other things: to designate one or more employees to coordinate the store's information security program; to identify internal and external security risks and to assess the sufficiency of any safeguards in place to control the risks; to design and implement reasonable safeguards to control the risks identified through the risk assessments; to regularly test and monitor the effectiveness of the safeguards; and to report twice a year for twenty years to the FTC regarding the steps that BJ's implemented to safeguard consumers' data. FTC Consent Order, <http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf>.

Unfortunately for BJ's, settling the FTC's complaint did not end its legal troubles. Some of the banks and credit unions that issued credit and debit cards to BJ's customers sued BJ's to recover the amounts they reimbursed cardholders for fraudulent purchases and to

recover the costs of reissuing cards. See Mary Kerwan, "The Weakest Link," *Globe & Mail Update* (July 4, 2005), <http://www.globetechnology.com/servlet/stories/RTGAM.20050704.gtkirwanju14/B&Sstory/einsider/> (describing Pennsylvania State Employees' Credit Union lawsuit against BJ's and its merchant bank, Fifth Third Bank, seeking more than \$98,000 incurred canceling and reissuing more than 20,000 cards). CUNA Mutual, representing 163 bond policy holders, is also suing BJ's and Fifth Third Bank. See *Credit Union Lawsuit Filed to Recover Costs Related to Security Breach Seen as Trend*, 4 Privacy & Security Law Report (BNA) 863 (July 4, 2005) (describing *CUMIS Ins. Soc'y Inc. v. BJ's Wholesale Club, Inc.*, No. 05-1158-J (Mass. Super. Ct., Apr. 4, 2005)). The claims in *CUMIS* include breach of contract, fraud, negligent misrepresentation, deceptive practices, and equitable subrogation. In a similar case, a federal court denied BJ's and Fifth Third Bank's motions to dismiss breach of contract, negligence, and equitable subrogation claims. See *Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, No. 05-CV-0021-P-S, 2005 WL 1610654, at *6 (D. Me. July 8, 2005).

II. The Increasing Threat To Consumer Data

Law enforcement agents report that the profile of computer criminals has shifted over the last few years from young hackers intent on drawing attention to their computer skills to profit-driven criminals. See *FBI Cyber Squads in Los Angeles See Increase in Computer-Related Crime*, 4 Privacy & Security Law Report (BNA) 983, 984 (July 25, 2005). The Los Angeles FBI office has 32 agents working full time on cyber-crime and those agents work with agents from the U.S. Secret Service, the Los Angeles Police Department, the Los Angeles County Sheriff's Department, the Los Angeles County District Attorneys Office, and the California Highway Patrol. *Id.* Law enforcement appears at this juncture, however, to be losing the battle against these cyber-thieves.

The viruses, worms, spyware, adware, and other such "malware" code that are surreptitiously downloaded onto computers are increasingly intended to steal valuable data. See Rochelle Shaw, *The Inside Story on Security Breaches*, CIO TODAY, Jan. 29, 2005, http://www.cio-today.com/story.xhtml?story_id=37480. Much surreptitiously downloaded malware now targets data held by businesses rather than data located on consumers' computers. *Id.*

The increased sophistication and ruthlessness of cyber-criminals have had predictable effects. A survey completed in September 2003 estimated that **9.91 million** persons in the United States suffered from identity theft in the preceding 12 months. Federal Trade Commission—Identity Theft Survey Report, <http://www.ftc.gov/os/2003/09/synovatereport.pdf>, at 7. The 2003 survey report estimated total losses to business and financial institutions at \$47.6 billion and to consumers at \$5 billion. *Id.* The report also estimated the average loss per victim was \$4,800 and estimated that each victim spent approximately 30 hours attempting to resolve the problems caused by thefts. *Id.* Another 2003 summary estimated that identity theft reports to agencies increased 177% from 2001 to 2002 and increased another 87.7% from 2002 to 2003. See *Identity Fraud—Analysis of Compelling Statistics*, <http://www.identitytheft911.com/education/fundamentals/idtheftstatistics.htm>.

In the first seven months of 2005, the personal information of more than **50 million** consumers has been lost or stolen. Eric Dash, *Europe Zips Lips; U.S. Sells Zips*, N.Y. TIMES, Aug. 7, 2005, at E1, available at <http://www.nytimes.com/2005/08/07/weekinreview/07dash.html>; and *A Chronology of Data Breaches Reported Since the ChoicePoint Incident*, <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (itemizing lists 66 incidents data breaches since February 15, 2005, that have exposed personal data of 50,476,170 individuals through hacking, loss of backup tapes and laptops, stolen laptops, compromised passwords, and dishonest insiders).

Some commentators believe that thefts of consumer data from businesses have been made public only because California Civil Code §§ 1798.29, 1798.82 and 1798.84 (sometimes referred to as "S.B. 1386," the title of the 2002 bill by which they were enacted) have required disclosure since July 2003 if California residents' data have been stolen. See *Former FTC Official Urges Congress to Avoid Hasty Data Security Legislation*, 4 Privacy & Security Law Report (BNA) 1009 (Aug. 1, 2005) (referring to comments by Marc Rotenberg, executive director of the Electronic Privacy Information Center). From April through mid-August, 2005, 14 additional states enacted consumer data breach notification statutes generally modeled on California's statute. The states are Arkansas (SB 1167); Connecticut (SB 650); Florida

(HB 481); Georgia (SB 230); Illinois (HB 1633); Indiana (SB 503); Minnesota (HF 2121); Montana (HB 732); Nevada (SB 347); New York (A. 4254); North Dakota (SB 2251); Tennessee (SB 2220); and Washington (SB 6043). The legislature of North Carolina has also passed such legislation but that bill has not yet been signed by the governor of that state. See *Data Security Breaches and Consumer Notification*, <http://www.bna.com/webwatch/databreaches.htm>.

It may never be determined whether recently reported instances of data theft are the tip of an iceberg that was concealed before California's data breach notification statute went into effect, or are caused by increasingly sophisticated cyber-thieves, or are due to both causes. It cannot be debated, however, that the number and costs of data thefts are rising dramatically.

III. Details Of Some High-Profile Data Thefts

Between November 2004 and February 2005, thieves obtained 1.4 million credit card numbers and the names on those accounts from 108 DSW shoe stores in 25 states. They also obtained checking account numbers and drivers' license numbers on 96,000 check transactions. Press Release, Attorney General Cox Issues Update on DSW Identity Theft, <http://www.michigan.gov/ag/0,1607,7-164-17278-116033--,00.html>. The Attorney General of the State of Ohio sued DSW seeking a declaratory judgment that the company is required by the Ohio Consumer Sales Practices Act to notify each of the consumers whose personal information was stolen. *State of Ohio v. DSW, Inc.*, No. 05CVH06-6128 (Franklin Cty. Ct. Com. Pleas, filed June 6, 2005).

Another type of data theft that was revealed in March 2005 was from a data broker, ChoicePoint, Inc. ChoicePoint is one of the largest data aggregators in the United States. It provides information not only to private business but also to various law enforcement agencies. A ring of data thieves led by Olatunji Oluwatosin (who later pleaded "no contest" to identity theft) initially convinced ChoicePoint that they were legitimate business people seeking to collect past due accounts from consumers. The theft ring purchased data regarding at least 145,000 people across the United States, including the individuals' social security numbers, property tax assessor file numbers, professional license numbers, vehicle registration numbers, bankruptcy records, and so forth. See *Choice-*

Point Data Security Breach, <http://www.privacyrights.org/ar/CPResponse.html>, and Robert O'Harrow Jr., *ChoicePoint Data Cache Becomes a Powder Keg*, WASH. POST, March 5, 2005, at A1, available at <http://www.washingtonpost.com/wp-dyn/articles/A8587-2005Mar4.html>. The theft ring used the information they obtained from ChoicePoint to open credit card accounts in the victims' names and to purchase large amounts of goods. *Id.* The theft ring was uncovered when a ChoicePoint employee became suspicious when Mr. Oluwatosin requested additional information over the telephone about a consumer and because some of the documents provided by Mr. Oluwatosin appeared to be fake. *Id.*

Law enforcement officials have determined that at least 750 people were victims of identity theft perpetrated by the theft ring led by Mr. Oluwatosin. Tim Gray, *ChoicePoint Data Theft Fallout Spreads to 145,000*, <http://www.internetnews.com/security/article.ehp/3484501>.

Another large scale theft from a data aggregator, Seisint, Inc., now a subsidiary of LexisNexis. Jonathan Krim and Robert O'Harrow Jr., "Data Under Siege," WASH. POST, May 10, 2005, at E1, available at <http://www.washingtonpost.com/wp-dyn/articles/a19982005Mar9.html>. LexisNexis discovered the theft in March 2005 after it bought Seisint and began reviewing Seisint's files prior to merging the data into existing LexisNexis files. LexisNexis officials discovered that thieves had obtained the IDs and passwords from legitimate customers and had used the data to obtain personal information about people in all 50 U.S. states. Antone Gonsalves, *ID Thieves Break Into LexisNexis Database*, TECHWEB NEWS, March 9, 2005, <http://informationweek.com/story/showArticle.jhtml?articleID=159400252>. LexisNexis eventually estimated that names, addresses, and social security and driver's license numbers, for as many as 310,000 people, had been exposed through the breach of Seisint's authentication protocols. Tim Gray, *310,000 Exposed by LexisNexis Data Breach*, April 12, 2005, <http://www.internetnews.com/security/article.php/3497111>.

In "the largest security breach to come to light so far," information regarding more than 40 million credit cards was stolen from CardSystems Solutions, Inc. *Latest Security Breach Exposes 40 Million Credit*

Card Accounts to Potential Fraud, <http://www.consumeraffairs.com/news04/2005/cardsystems.html>. CardSystems is a Tucson, Arizona-based company that processes credit and debit card payments for banks and merchants. MasterCard International first revealed the breach and blamed the theft on a single individual. *Id.* MasterCard said that the criminal used "a virus-like computer script that captured customer data." *Id.* It is unclear when CardSystems or the credit card companies first became aware of the problem. CardSystems officials say that they first noticed a potential security breach on May 22, 2005, and contacted the FBI the following day. *Id.*

A putative class action has been filed against CardSystems, a bank, Visa and MasterCard. *Parke, et al. v. CardSystems Solutions, Inc., et al.*, No. CGC-05-44264 (S.F. Cty. Super. Ct.). A copy of the First Amended Complaint in that action, filed July 6, 2005, is available at <http://www.techfirm.com/cardsystems.pdf>. The Amended Complaint alleges that CardSystems was negligent and breached California's data protection statute in several ways, including by failing to take reasonable steps to destroy customer records when they were no longer needed, by failing to take reasonable security measures to protect personal information, by failing to encrypt the personal information, and by failing to timely inform consumers of the security breach. The Amended Complaint seeks both damages and injunctive relief.

On August 2, 2005, the court granted a temporary restraining order and order to show cause against the defendants in the *CardSystems* case. The order prevents them from destroying records regarding the security breach and orders them to show why they should not be required to notify all California residents whose payment card information was accessed (which plaintiffs claim they have failed to do), should not be ordered to immediately implement and maintain compliance with the Payment Card Industry Data Security Standards, and should not be ordered to continue to maintain data regarding the data breach. "Temporary Restraining Order and Order to Show Cause Re: Preliminary Injunction," ¶¶ 2-3, 5.

IV. Lawsuits Against Credit Card Issuers Have Been Unsuccessful

It is not surprising that the plaintiffs in *Parke v. CardSystems Solutions, CUMIS Ins. Soc'y BJ's Wholesale*

Club, and *Banknorth v. BJ's Wholesale Club* are suing the companies from which data were stolen and their merchant banks rather than attempting to recover from the banks that issued credit cards to identity thieves. Prior cases against banks for issuing cards or extending existing credit to identity thieves have been uniformly unsuccessful.

The court in the leading case, *Polzer v. TRW, Inc.*, 682 N.Y.S.2d 194 (App. Div. 1998), held that "New York does not recognize a cause of action for 'negligent enablement of imposter fraud,' and that plaintiffs otherwise failed to state a cause of action in negligence . . ." The court affirmed summary judgment dismissing the victims' claims against an issuing bank and a credit agency.

Polzer was followed in *Huggins v. City Bank, N.A.*, 355 S.C. 329, 585 SE.2d 275 (S.C. S. Ct. 2003), where the court held that identity theft victims had no tort claim against banks that had issued credit cards to unknown imposters. *See also Watson v. Trans Union Credit Bureau*, No. CIV:04-205B-C, 2005 WL995687 at * 1 (D. Me. April 28, 2005) (magistrate recommends dismissal of state law negligence claims as preempted by federal Fair Credit Report Act); and *Vasquez-Garcia v. Trans Union de Puerto Rico*, 222 F. Supp.2d 150 (D. Puerto Rico 2002) (finding victims' state law claims against issuer for negligently issuing credit card preempted by FCRA).

Some commentators have urged courts to accept negligence claims against card issuers. *See, e.g., Anthony E. White, The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Whose Going to Pay for It?* 88 Marq. L. Rev. 847, 865 (Spring 2005). There is no indication courts are inclined to follow this advice.

V. Pending Litigation Tests The Effectiveness Of State Data Protection Laws And New Legal Theories

California Civil Code § 1798.81.5(b), which was added to California's data protection statutes in 2004, provides in part: "[a] business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or

disclosure.” The first and second causes of action in the *Parke v. CardSystems Solutions* Amended Complaint rely on this provision of the California Civil Code. Another section of the same chapter, Section 1798.81, requires businesses to “take all reasonable steps to destroy, or arrange for the destruction of a customer’s records within its custody or control containing personal information which is no longer to be retained” The third cause of action in *Parke* Amended Complaint relies on this provision. Yet another provision of the California statute, § 1798.82, requires that businesses notify California residents when the residents’ personal data are “reasonably believed to have been acquired by an unauthorized person” the fourth cause of action relies on this section.

The fifth cause of action in the *Parke* Amended Complaint relies on common law negligence but alleges that the defendants “assumed the duty to use reasonable care to keep the credit card account and other non-public information of the Consumer Class . . . private and secure.” This allegation relies on the Payment Card Industry Data Security Standards to supply the duty of reasonable care that was found wanting in previous cases against issuers of credit cards to identity thieves. The plaintiffs in the *Parke* action also seek damages under California business and professions code §§ 17200, *et seq.*, which provide causes of action for unfair practices by California businesses. Finally, the plaintiffs in *Parke* seek a declaratory judgment that the defendants breached the various California statutes at issue and seek injunctive relief.

The reliance of the *Parke* plaintiffs on the California data protection and data breach statutes will provide a vehicle to determine whether these statutes are effective. The *Parke* plaintiffs at least have the advantage of relying on legal theories that have not previously been rejected by other courts.

Similarly, the plaintiffs in *Banknorth v. BJ’s Wholesale Club* are relying on the Visa Operating Regulations (the predecessor regulations to the Payment Card Industry Data Security Standards). The plaintiffs in *Banknorth*, however, have pleaded their claims as breach of third party beneficiary contract duties allegedly owed to the plaintiffs, as well as negligence and equitable subrogation claims. The first and last claims, have not previously been rejected in this context. The court’s ruling denying the defendants’ mo-

tions to dismiss on July 8, 2005, suggests that, at the very least, the defendants will have to engage in some discovery before the claims are resolved.

The claims in these lawsuits make it clear that businesses that process consumer data of any kind should follow the Payment Card Industry Data Security Standards, which are mandatory for institutions that process bank card data. A copy of the standards, which are both thorough and concise, are available at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf.

The outcome of the *Parke*, *Banknorth*, and *CUMIS Ins. Soc’y Inc* cases will help determine whether state data breach notice laws and the theories that rely on payment card industry data security standards and regulations will finally enable identity theft victims, and banks that are required to reimburse fraud victims and re-issue cards, to be compensated for their damages. Even if the plaintiffs in the *Parke* cases are successful, however, federal legislation could prevent other victims from relying on state data breach laws.

VI. Federal Law Legislation May Preempt Claims Such As Those Pleaded In *Parke v. CardSystems Solutions*

On July 28, 2005, the Senate Commerce Committee passed a substitute version of S. 1408, the “Identity Protection Act.” Press Release, Senate Commerce Committee, <http://commerce.senate.gov/newsroom/printable.cfm?id=242027>. The substitute bill includes national notification standards (Section 3), allows the FTC and state attorneys general to enforce the law (Sections 5 and 6), preempts state laws (Section 7), and states that “[n]othing in this Act establishes a private cause of action against a covered entity for violation of any provision of this Act.” (Section 5(f)). See <http://commerce.senate.gov/pdf/s1408sub5.pdf>.

There are numerous other federal bills pending, both in the House and in the Senate, that address the same topics. It is unclear at this time whether substitute S.1408 or any other proposed federal data protection legislation will be enacted. If, however, substitute S. 1408 or any other federal bill that preempts state data protection laws and precludes private lawsuits is signed into law, future claims such as those in *Parke v. CardSystems Solutions* that rely on state data breach notification laws will be precluded. Such preemption

may not, however, affect consumers' and payment card issuers' claims for breach of contract and equitable subrogation.

VII. Conclusion

Data thieves will continue to plague businesses that process consumers' personal information.

Such businesses must implement comprehensive security measures to thwart as many data thefts as possible and to improve their odds of defeating consumers' and payment card issuers' claims in the lawsuits that will be filed whenever thieves succeed in stealing large amounts of consumer data. ■