Who Should Pay the Price for *Identity Theft?*

The answer to this question appears to be straightforward; obviously, it should be the criminal fraudster responsible for committing the identity theft-related fraud. All too often, however, the fraudsters are not caught; or if they are, there are no funds left to recover. Under current law, financial institutions (FIs) that issue the debit or credit cards often ultimately wind up footing the bill for both fraud related losses and costs of issuing new cards and/or accounts for their customers. FIs are increasingly concerned that data security breaches where hackers or fraudsters steal the "personally identifiable information" necessary to commit identity theft fraud are causing the FIs to suffer more fraud-related losses. The data security breach incident reported by TJX Companies in early 2007 may mark the beginning of a shift in allocation of such fraud-related losses. In addition to consumer class action complaints filed against TJX Companies over the data breach incident, FIs have also filed class action lawsuits targeting retailer and processor liability for data security. FIs have also been involved in lobbying efforts designed to statutorily shift fraud losses and associated costs away from FIs to the entities actually responsible for the data security breach. A legal fight is brewing in both the courts and legislatures over who will ultimately bear the losses of identity theft-related fraud.

By Erin Fonté

Five years ago, if you asked the average person on the street to identify his or her top concerns, only a small percentage would have listed financial fraud resulting from identity theft. Times have changed, however; in a recent study by Zogby Interactive, a vast majority of respondents (91 percent) reported being concerned that their identity might be stolen and used to make unauthorized purchases.[1] Of that 91 percent, 50 percent said they were "very concerned." These survey results are not surprising in light of the proliferation of identity theft and related financial fraud as well as the media coverage of data security breaches that can, and in some cases do, give rise to such identity theft and fraud.

The level of concern about identity theft is understandable, given the dollar amounts at stake. A March 2007 study from Gartner found that from mid-2005 until mid-2006, about 15 million Americans were victims of fraud stemming from identity theft—an increase of more than 50 percent from the estimated 9.9 million victims reported in 2003.[2] The total one-year fraud amount for 2006 is estimated at $55.7 *billion*,[3] and the average number of hours each victim devotes to resolving fraudulent transactions and negative credit reporting issues is thought to be 40 hours per victim.

Consumers harmed by identity theft-based fraud must spend a great deal of time, effort, and money to report and resolve fraudulent transactions, but the financial institutions (FIs) backing the bank accounts, debit cards, and credit cards often bear the brunt of the actual loss attributable to fraudulent transactions. Under federal laws governing FIs and credit card companies, FIs must generally cover most, if not all, losses resulting from identity theft-based financial fraud. FIs that hold the consumer's financial accounts and issue debit cards associated with those accounts or credit cards must generally bear the costs of opening and closing accounts; deposits, transactions, and other payments tainted by the fraud; canceling and reissuing cards (both debit cards and credit cards, as applicable); and refunding fraudulently charged amounts or crediting consumers for unauthorized transactions in accordance with applicable law and rules governing credit cards.

Both state and federal laws generally prohibit identity theft itself as well as the various types of identity theft-based offenses committed via the use of stolen "personally identifiable information" (PII).[4] Victims of identity theft can file police reports regarding their losses. The financial institutions that are affected generally work with law enforcement to help track down and catch the perpetrators, and such institutions can take action as allowed under law to recoup lost funds stolen by fraudsters and other criminals. But all too often, the stolen funds have been transferred to institutions outside of the country or otherwise have been disposed of or converted before the thief is caught. Law enforcement agencies and prosecutors have become increasingly sophisticated in bringing many fraudsters to justice, but identity theft still remains a crime that pays because it can be perpetrated "behind the shadowy cloak of a computer keyboard. … You don't event need to be in the same city or country as your victim. … You can steal someone's identity without being able to speak his language or pronounce her name."[5] Moreover, investigations are increasingly revealing that many identity theft activities are orchestrated and carried out by organized crime rings. In addition, in many instances the crime has two distinct components carried out by two separate and unaffiliated individuals or organizations.

As with any cost, FIs often offset such losses by increasing fees, and FIs may even be able to mitigate some of their losses via insurance coverage. Still, the dollar losses due to identity theft-based fraud represent vast dead-weight economic losses borne by FIs. And with the increase in the number of reports of data security breaches, FIs have begun to notice a common thread among the fraudulent activities. The vast majority of data security breaches involving PII does not originate with FIs but, rather, with government entities, universities and other higher education institutions, retailers (where many day-to-day credit card and debit card transactions occur), and lightly regulated third-party transaction "processors" that aid in routing and processing the credit card and debit card transactions. Fraudsters look for the weakest security in the flow of financial and transactional data so that they can reach into that stream of information to extract the data they want.

On Jan. 17, 2007, TJX Companies (TJX), the parent company of retail chains T.J. Maxx, Marshalls, HomeGoods, and A.J. Wright, announced that an unauthorized intruder had accessed TJX's computer systems that process and store information related to customer transactions for its retail stores, including detailed information about customer debit and credit cards.[6] According to subsequent reports, the number of credit and debit cards that were exposed in this incident reached at least 45 million.[7]

This particular data breach incident could spur a shift in thinking among FIs about identity theft-based fraud. To date, at least 18 separate lawsuits have been filed against TJX stemming from this breach, including two class action suits to hold TJX responsible for the losses the FIs suffered. In addition, legislative efforts are under way in at least seven states that would mandate that negligent retailers pay the costs of the remediation measures that FIs have to take to protect their customers, including dollar losses incurred by FIs because of identity theft-based fraud. Minnesota recently became the first state to enact a law dealing with this issue.

The FIs essentially take the position that unregulated retailers and other entities that do not employ adequate security measures to protect their customers' personally identifiable information should pay the costs of such shoddy security practices. For example, most major retailers have implemented Payment Card Industry Data Security Standards (PCI DSS) to protect credit card data, but only about 19 percent of smaller retailers are in compliance.[8] As a result of fallout from the TJX data security breach, FIs have recently unleashed a series of lawsuits and lobbying efforts aimed at shifting the liability and costs associated with identity theft-based fraud losses to the entities—including retailers—responsible for data security breaches.

This article provides a brief overview of the issues in-

volved in identity-based fraud and the relevant laws apportioning the risk of loss among FIs and credit card associations. In addition, this article will describe the legal fight brewing in both the courts and state legislatures (and potentially the U.S. Congress) over who is to blame for the loss of PII and who should be held responsible for the costs of identity theft-based fraud potentially tied to data security breaches of PII.

What Is Identity Theft, and How Is It Committed?

The ultimate goal of the perpetrators of identity theft is to gain enough information to access a victim's money and/or good credit. Frank Abagnale, a notorious check-fraudster whose story was told in the movie "Catch Me If You Can," became a consultant to financial institutions, law enforcement agencies, and other institutions after he was apprehended and served his sentence. In his book, *Stealing Your Life*, Abagnale made the following observations about identity theft:

> I know cons, and right away I saw that this one was going to be the sweetest of all. For the past 32 years, ever since forsaking my foolish teenage infatuation with perpetrating swindles, I've been a professional expert in how to prevent fraud. … Years before I would never have guessed that [this crime] could even be invented, for it was the most incredible but also the simplest crime ever perpetrated. This festering crime is what we now know as identity theft, the wholesale lifting of someone's identity for illicit gain. It's stealing that identity, then using it to access a person's bank account, their personal information, and their personal finances. It's becoming someone else for the bucks.[9]

Identity theft can start with lost or stolen wallets, pilfered mail, data security breaches, computer viruses, or rifling through paper documents thrown out by individuals or businesses ("dumpster diving"). In addition, as described below, fraudsters use increasingly advanced methods for accessing PII, including "phishing," "pharming," "shoulder-surfing," and "skimming."

Phishing

Phishing allows a fraudster to acquire information—such as user names, passwords, and credit card details—by masquerading as a trustworthy entity in an e-mail or other electronic communication. Frequent targets of phishing attacks have included eBay and PayPal, as well as the Web sites of online banking and financial services. Phishing is typically carried out by e-mail or instant messaging, and often the fraudster's e-mail communication instructs users to type in PII details at a Web site (although telephone calls have also been used in phishing attacks). Phishing also often employs "Web page spoofing," whereby a legitimate Web page, such as an FI's online banking Web site, is reproduced on another server that is under the control of the fraudster, who then captures the customer's PII when he or she attempts to log in.

Many FIs now combat phishing attacks through the use of sophisticated security procedures and anti-phishing programs. FIs have also aggressively educated their customers about ways to distinguish legitimate FI e-mails from fraudulent ones. In recent years, new legislation has made phishing a crime, and more businesses (in addition to FIs) have begun to use customer training and to employ sophisticated anti-phishing software.

Pharming

Pharming is a different type of fraudster attack designed to redirect a Web site's traffic to another site that is a bogus site. Pharming "poisons" a domain name server (DNS) by infusing false information into the DNS, redirecting the user elsewhere even though the user's Web browser displays the intended Web address. Pharming is more difficult to detect than phishing, because all the information from the user's end shows a connection to the legitimate Web site that the user intended to contact. Pharming has become a major concern to businesses hosting e-commerce and online banking Web sites. Protection agains this serious threat requires sophisticated anti-pharming measures; antivirus and spyware removal software cannot necessarily protect against pharming.

Shoulder-surfing

The term "shoulder-surfing" refers to a low-tech fraudster attack using direct observation techniques, such as looking over someone's shoulder, to obtain sensitive PII. Shoulder-surfing is particularly effective in crowded places, such as stores and shopping malls, where fraudsters can simply stand next to someone and watch that person fill out a form and enter a PIN number or a password. Shoulder-surfing can also be done at a distance, with the aid of binoculars or other vision-enhancing devices. In addition, inexpensive miniature closed-circuit television cameras can be concealed in ceilings, walls, or fixtures and data entry can be observed through these devices.

The first line in combating shoulder-surfing attacks, of course, is for individuals to shield their information (PIN number entry activities and the like) from prying eyes. However, new ATMs now employ advanced screen displays that discourage shoulder-surfers; the screen grows darker at a certain angle and the only way to tell what is being entered on the screen is to stand directly in front of it. Certain models of credit card readers have recessed keypads and rubber shields that surround a significant part of the keypad opening. Consumer diligence and these new technological measures can decrease incidences of shoulder-surfing, but this is still one of the easiest ways for a fraudster to get access to PII.

Skimming

Fraudsters can skim the credit or debit card numbers and PINs used in regular retail store transactions by either swapping out a standard point-of-sale (POS) terminal for one that includes a skimming device or modifying a normal POS terminal by attaching a skimming device directly to the terminal. In early 2007, four men were arrested and ar-

raigned on charges of stealing money from the FI accounts of customers of a Stop 'N Shop in Coventry, R.I.[10] Video surveillance showed the four men leaving after allegedly replacing the store's POS terminals with their own terminals. Police investigating this incident believe that the suspects also targeted stores in Cranston, Providence, Bristol, and Warwick, R.I., and may be involved in similar incidents in Las Vegas, Miami, Atlanta, Philadelphia, and Richmond, Va. Law enforcement officials also believe that the suspects may be part of an international organized crime ring. The major advantage fraudsters gain by using skimming techniques is that they can sometimes get information on thousands of cardholders by skimming on only one or two POS terminals.

Where Do Fraudsters Steal Information To Commit Identity Theft?

Fraudsters will generally steal PII from whatever business or entity they can infiltrate to get the information. Numerous colleges and universities have reported data security breaches involving, at a minimum, the names and social security numbers of students and former students. Several FIs have also reported data security breaches ranging from the theft of laptop computers containing unencrypted personal information to unencrypted data tapes falling off document delivery trucks. In recent testimony before the U.S. Judiciary Committee, Joanne McNabb, the chief of the California Office of Privacy Protection, reported the results of her office's survey of 530 data security breaches that have occurred since 2003.[11] Of these incidents, colleges and universities accounted for 28 percent of the breaches; government agencies (federal, state, and local), approximately 24 percent; financial services, 14 percent; medical facilities, 11 percent; retail establishments, 5 percent; and elementary and secondary schools, 5 percent. Manufacturers, data brokers, and other businesses accounted for the remaining 15 percent. Even though there are connections between data security breaches involving PII and the use of PII to commit identity theft, to date there are no conclusive studies about the correlation between data security breaches and whether information from a particular data security breach is actually used to commit identity theft or the rate at which stolen PII is successfully used to commit identity theft.[12]

Who Bears the Costs of Identity-Theft Based Fraud?

Financial Institutions and Electronic Transfers

For many years, the security of PII and financial information was largely the responsibility of FIs (banks, credit unions, savings and loan institutions, and so forth), credit reporting bureaus, and credit card companies. These entities are subject to many rules and regulations regarding privacy and security of PII and requiring FIs to make consumers whole in cases of financial fraud.

The federal Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA),[13] opened up competition among traditional FIs, securities companies, and insurance companies. The GLBA also includes provisions to protect consumers' personal financial information held by FIs. There are three principal parts to the GLBA privacy requirements: the Financial Privacy Rule, the Safeguards Rule, and pretexting provisions.

The Financial Privacy Rule

The Financial Privacy Rule[14] governs the collection and disclosure of customers' personal financial information by FIs. The rule also applies to companies, whether or not they are FIs, that receive such information. FIs must issue and annually update a privacy notice explaining what information is collected about the consumer, with whom such information is shared, how it is used, and how it is protected. The privacy notice must also identify the consumer's right to prohibit sharing his or her PII[15] with unaffiliated parties, as provided for by the Fair Credit Reporting Act.

The Safeguards Rule

The Safeguards Rule[16] requires all FIs to design, implement, and maintain safeguards to protect customer PII. The Safeguards Rule applies not only to FIs that collect PII from their own customers but also to entities—such as credit reporting agencies—that receive customers' PII from other FIs. The Safeguards Rule requires FIs to develop a written information security plan detailing what procedures and mechanisms the FI employs to protect customers' PII on an ongoing basis. The Safeguards Rule also applies to any PII of former customers of the FI that the institution maintains. An FI's data security plan must include the following steps:

- designating at least one employee to manage the data protection safeguards;
- constructing a thorough risk management profile for each department within the FI handling the PII;
- developing, monitoring, and testing a program to secure the PII; and
- changing the data protection and safeguards as needed with the changes in how PII is collected, stored, and used.

The Safeguards Rule generally forces FIs to take a closer look at how they manage PII and to perform a risk analysis on their current processes.

Pretexting

The pretexting provisions of the GLBA protect consumers from individuals and companies that obtain their PII under false pretenses, a practice known as pretexting.[17] Pretexting (sometimes referred to as "social engineering") occurs when someone tries to gain access to PII without proper authority to do so, often by impersonating the account holder by phone, mail, or e-mail. The GLBA has provisions that require the FI to take all precautions necessary to protect and defend the consumer's PII from all varieties of pretexting efforts.

In addition to the GLBA's provisions, FIs are also subject to the federal Electronic Funds Transfer Act (EFTA), which generally governs electronic transfers, including

debit card and ATM transactions.[18] In implementing the EFTA, the Federal Reserve Board promulgated Regulation E, which lists the rights, liabilities, and responsibilities of participants in electronic fund transfer (EFT) systems, such as ATM transfers, telephone bill-payment services, POS terminal transfers, and preauthorized transfers from or to a consumer's account (such as direct deposits and social security payments).

Regulation E imposes limitations on the financial liability of consumers for an unauthorized EFT resulting from loss or theft of an EFT "access device." If the consumer's "access device and secret code" (that is, card and PIN number) are lost or stolen and the consumer notifies the FI prior to any unauthorized transfers, the consumer may avoid monetary loss. After receiving the report of the loss or theft, the FI typically switches off the access device and issues a new one or may even close the consumer's old account and open a new one.

If, in the same situation, the perpetrator makes an unauthorized EFT but the consumer notifies the FI within two business days of discovering the EFT, then the consumer's loss is generally limited to the amount of the unauthorized EFT, up to a maximum of $50. If the consumer waits more than two business days after learning of the unauthorized EFT to report it, however, then the consumer may be liable for losses up to a maximum of $50 for the losses suffered within the first two business days, *plus* an additional $500 if the FI can establish that the loss would not have occurred if the consumer had notified the FI within the first two business days. In addition, a consumer can also lose this $500 liability limitation if he or she waits more than 60 days from the date on which the account statement showing the unauthorized EFT is mailed or otherwise transmitted to the consumer. However, given the way the Regulation E provisions work, most individuals who suffer unauthorized EFTs related to debit cards and/or ATM cards generally lose no more than $50 if they notify their FI.

Credit Card Associations and Credit Card Transactions

The use of credit cards is governed by a different set of laws but, in general, these laws also provide for consumer protection in the event of fraudulent purchases. Under the provisions of the Fair Credit Billing Act,[19] consumers generally have zero liability for fraudulent purchases when they can provide evidence of fraud. The credit card associations operate via a collection of contracts between the FI issuing the credit cards (the issuing FIs), any third-party processors responsible for processing credit card transactions, and merchants that accept the credit cards for payment. Generally, the operating rules of the credit card associations require the issuing FIs to implement the "zero liability" policy for fraudulent credit card charges, and thus the issuing FIs ultimately must absorb the costs of such fraudulent charges.

The credit card associations have also implemented data security standards for merchants and transaction processors that are part of the respective card networks. The newest version of these security standards, mentioned above, is the PCI DSS. The PCI DSS were created by five major credit card companies—Visa International, MasterCard Worldwide, American Express Co., Discover Financial Services LLC, and Tokyo-based JCB Co.—to protect credit card data before, during, and after transactions.[20] Merchants were required to implement the new PCI DSS standards by 2005, but the percentage of small merchants that are PCI DSS-compliant remains low—about 18 percent. The PCI DSS (similar to the Cardholder Information Security Program) generally prohibits merchants from "retaining and storing magnetic-stripe data" from a card after the POS transaction has been completed.

Current Allocation of Financial Liability for Fraud

The allocation of financial liability for identity theft-based fraud falls heavily on FIs. Even though the FIs can generally raise certain fees charged to customers or merchants, the FIs still bear a great deal of the costs of the fraudulent transactions, along with attendant costs of responding to data security breaches (such as closing and re-opening potentially compromised accounts or issuing new debit/ATM and credit cards). The FIs on the back end of processing and settling electronic funds and credit card transactions are subject to extensive examinations and rules, including strict privacy and security requirements. However, retailers and merchants on the front end of electronic funds transfers and credit card transactions, as well as other government and educational entities and businesses that store PII, are lightly regulated or unregulated and, in the view of many FIs, are falling down on the security front and creating security weaknesses in the financial transaction data stream.

Despite protestations from many businesses (especially small businesses) that the costs of increased security requirements could place enormous financial burdens on them, FIs are responding to the TJX security breach with an "enough is enough" attitude. For the first time a concerted industry effort is now under way to shift at least some liability from FIs to those parties arguably responsible for the breaches. This effort is occurring on both the judicial and legislative fronts.

Overview of Court Cases Regarding Data Security Breach Liability

The case law governing data security breaches is understandably sparse, given that reports of such breaches date only to 2003. In one recent Minnesota case, however, the plaintiff lost a tort claim for damages against a financial loan services company that suffered a data security breach.[21] In that case, the Brazos Higher Education Service Corporation, a provider of student loans, faced a lawsuit after an employee's laptop computer, which contained unencrypted PII for roughly 550,000 customers of the company, was stolen from his home. Although none of the information was reportedly used to defraud any Brazos customer, one customer, Stacy Guin, sued Brazos for negligence, alleging the following:

- Brazos owed Guin a duty to "secure private personal

information and not put it in peril of loss, theft or tampering";
- Brazos breached the duty; and
- Guin was damaged as a result.

Guin claimed that, because Brazos is a financial institution, the GLBA requires the company to ensure the "security and confidentiality of customer records and information" from foreseeable and anticipated threats.

Guin argued that Brazos breached the statutory duty imposed by the GLBA. The court determined, however, that Brazos had adequate written security policies and risk assessment reports in place and used sufficient safeguards to prevent acquisition of its customers' information. Moreover, the court found that Brazos was in compliance with the GLBA, which neither requires specific safeguards nor mandates that all personal information be encrypted, according to the court. Rather, the court ruled, the statute merely requires "reasonable measures to protect [personal] data" from foreseeable risks and, in the court's opinion, Brazos had implemented such measures.

Guin argued that the theft of the laptop computer was reasonably foreseeable, because allowing PII to remain unencrypted on an unsecured computer increases the risk of theft. In addition, Guin noted that this particular theft was foreseeable because of the company's knowledge of similar thefts in the financial industry. The court concluded, however, that the Brazos employee himself was not aware of any previous burglaries in his block or in his immediate neighborhood, and therefore "[t]here is no indication that [the Brazos employee] or Brazos could have possibly foreseen the burglary which took place on September 24, 2004."[22] The court also pointed out that there was no evidence that a third party had gained access to any PII. It is unclear whether courts analyzing a similar negligence claim in the future would issue a ruling similar to the one rendered in the *Guin* case, particularly given changing industry practices and standards regarding encryption of PII.

In another case focusing on transaction processing requirements, the plaintiff, Sovereign Bank, incurred losses when its customers' credit card numbers and associated account information were stolen from the computer databases of BJ's Wholesale Club.[23] The security breach occurred between July 2003 and February 2004, and after discovery, Visa notified all individuals whose PII and card information was potentially compromised. Sovereign Bank brought claims against BJ's Wholesale Club and its transaction processor, Fifth Third Bank.[24] As previously discussed, Visa has implemented operating regulations that govern all members participating in the Visa system (FIs that issue credit cards, third parties or FIs that serve as card transaction processors, and merchants who accept Visa cards) as well as information security requirements to protect cardholders' data. Both the Visa operating regulations and the card data security requirements prohibit merchants from retaining and storing magnetic-stripe data from a credit card after the POS transaction has been completed. Sovereign Bank alleged that Fifth Third consistently retained and stored the magnetic-stripe data after transactions were completed in violation of the operating rules and card data security requirements.

Sovereign claimed that, because Fifth Third had violated the contract with Visa (via the operating rules), Sovereign could recover damages against Fifth Third as a third-party beneficiary to the Visa contract. The court determined, however, that Sovereign was merely an incidental beneficiary of the contract and would receive a benefit from the prohibition on the retention of magnetic-stripe data, but that alone was insufficient to make Sovereign an intended beneficiary. Instead, the court found that the operating instructions were intended to benefit the Visa system as a whole and not the specific entities (such as Sovereign) participating in the system. Therefore, Sovereign could not step into Visa's shoes to enforce the operating regulations.

These two cases are important, because they highlight many of the claims and issues alleged in the numerous other cases (approximately 18) currently filed against TJX. In *Mace v. TJX Companies Inc.* (filed Jan. 29, 2007), the plaintiff, Paula Mace, claimed that she had shopped at T.J. Maxx in December 2006 and was notified in January 2007 that her financial information had been compromised because of the corporation's data security breach incident.[25] The plaintiff class consists of other consumers, like Mace, whose personal and financial data had been exposed by the breach. The claim is based on a theory of common law negligence; according to Mace, TJX owed a duty to exercise reasonable care to safeguard all PII in TJX's possession. In addition, Mace alleges that the PII was "improperly stored and inadequately safeguarded in violation of … industry rules and regulations." Under this theory, using credit card industry standards and regulations as the standard of care, TJX breached its duty by failing to comply. The plaintiffs also argue that TJX had a special fiduciary duty to the class members (who entrusted TJX with valuable PII), that TJX had a duty to protect the plaintiffs' right to privacy, and that TJX had a duty to disclose the breach in a timely manner.

Mace claims that TJX breached all these duties, and the class members suffered damages—including fraudulent charges, loss of financial and personal information, and so forth—as a proximate result of the breach. Although it is unclear how the court will rule in this case, the central issue is likely to be the extent of the duty TJX owed to its customers. Is TJX subject to GLBA? If so, did TJX have adequate security procedures in place? Another central question will be whether the breach and its consequences were foreseeable.

TJX also faces suit from a group of FIs in *AmeriFirst Bank v. TJX Companies Inc.* (filed Jan. 29, 2007). According to reports of the TJX breach, many banks and FIs have reported stolen credit cards and fraudulent charges stemming from the TJX breach incident, with fraudulent activity occurring in Florida, Georgia, and Louisiana as well as overseas.[26] The breach exposed credit card and debit card information, driver's license data, and checking account information "linked to transactions for returned merchandise."[27]

AmeriFirst Bank brought a class action suit on behalf of itself and similarly situated FIs against both TJX and Fifth

Third Bank (the third-party transaction processor for TJX). The plaintiffs filed claims of negligence, breach of contract, and negligence per se. First, the plaintiffs claim that the defendants were negligent in that they breached the duty of care and unreasonably delayed reporting the security breach to consumers. Second, as in the *Sovereign* case, the plaintiffs' claim that they are third-party beneficiaries of the agreements between the defendants and credit card associations and can therefore enforce the agreement against the defendants. Third, the plaintiffs allege that the defendants are covered entities under the GLBA, and the defendants' failure to comply with the statute's requirements or industry standards constitutes negligence per se.

When evaluating the contract claim, the court may look to the Pennsylvania case involving BJ's Wholesale Club as persuasive authority that AmeriFirst and other banks are not intended third-party beneficiaries of the contracts between merchants and credit card associations. The third claim, however, raises the critical and novel issue of whether Fifth Third and TJX are "financial institutions" covered by the GLBA with respect to Fifth Third's activities in processing transactions and TJX's role as a retailer initiating such transactions.

The GLBA defines a "financial institution" as any institution that engages in financial activities described in 12 U.S.C. § 1843(k). This provision also brings within the statute's ambit several classes of activities that are financial in nature[28] under Regulation Y, which provides an extensive list of such nonbanking activities. Regulation Y classifies data processing and data transmission services (as long as the data are financial, banking, or economic in nature) as "financial" in nature, which would seem to include Fifth Third, the processor for TJX's credit and debit card transactions.

In contrast to Fifth Third, TJX is the parent company of a large conglomerate of retail stores and arguably does not engage in any activities covered by the GLBA. TJX's operations as a retailer may not be considered financial in nature under the categories listed in U.S.C. § 1843(k)(4) or Regulation Y. Furthermore, according to *American Bar Association v. Federal Trade Commission*,[29] Regulation Y was promulgated to identify nonbanking activities so closely associated with financial activities that they "may be engaged in by a bank holding company or its subsidiary in accordance with the requirements of [the] regulation." Therefore, the court may ultimately decide that, because the business activities of TJX (operating retail chains) are not closely related to traditional banking activities, TJX is not a covered financial institution under the GLBA.

The Massachusetts Bankers Association (MBA) filed a separate class action suit against TJX on April 25, 2007,[30] outlining five claims: (1) negligent misrepresentation, (2) unlawful and deceptive acts and practices in violation of Massachusetts law, (3) violation of the GLBA and unlawful and deceptive acts and practices in violation Massachusetts law, (4) negligence, and (5) breach of contract. MBA first claims that TJX, by participating in the Visa and MasterCard systems, represented that it would comply with the applicable operating regulations imposed by the credit card associations on any entity participating in the systems. In addition, MBA maintains that TJX knew or should have known that it was not in compliance with the rules—specifically the rules prohibiting retention, storage, or disclosure of the magnetic-stripe information obtained from customers' credit and debit cards. The class member FIs, the complaint reads, justifiably relied on the representation that TJX was in compliance with the card association operating regulations, including card data security requirements, and suffered damages as a result. Second, according to the complaint, TJX misrepresented its compliance with the operating regulations and failed to safeguard customers' data, constituting deceptive acts and unfair trade practices under Massachusetts law (TJX is headquartered in Massachusetts).

Third, MBA alleges that the GLBA imposes a duty on TJX "not to misuse or inappropriately disclose information" of customers. By storing the magnetic-stripe information, TJX "maintain[ed] the data well beyond the permitted timeframe" and "allow[ed] the data to be accessed by others for purposes unrelated to the processing of the credit or debit transaction." Finally, the complaint argues that the breach of the GLBA is also a violation of Massachusetts' unfair and deceptive trade practices statute (a claim that similar to the claim raised in the *AmeriFirst* case discussed above).

The final two claims assert negligence and breach of contract theories. The negligence claim alleges that TJX had a duty to provide "adequate" security to customers, and TJX breached this duty by allowing an unlawful intrusion into its system. Finally, similar to the *Sovereign* and *AmeriFirst* claims, MBA claims to be a third-party beneficiary of the agreement between TJX and the credit card operators.

The claims pending against TJX—especially those filed by the FIs—may have a significant impact on the allocation of liability for data security breaches and associated identity theft-based fraud. However, many FIs are not waiting for the outcome of these and similar cases. Instead, they are pursuing lobbying efforts to shift the allocation of liability via statute.

Overview of Legislative Attempts to Shift the Financial Liability for Data Security Breaches and Related Fraud

In seven state legislatures, bills were introduced in 2007 to shift the allocation of liability and costs associated with data security breaches. As of the writing of this article, three of those bills have died, three are still pending, and one was enacted. Minnesota became the first state in the United States to enact legislation that would shift costs and liabilities from FIs to the entities responsible for the data security breaches.

California

California Assembly Bill 779 is the mildest of the legislative measures in terms of the costs and liabilities the bill would shift away from FIs. The bill would clarify that retailers are subject to California data security breach notice requirements (although those entities are arguably already

covered under current law) and would prohibit covered persons or entities from maintaining, storing, retaining, or failing to limit access to customer data after a transaction (which would essentially codify a good portion of the PCI DSS requirements in the California statute).[31]

In contrast to the broader expense reimbursement provisions of legislation proposed this year in Connecticut, Illinois, Massachusetts, Minnesota, New Jersey, and Texas, the California bill's reimbursement requirements would apply only to the cost of the notice itself in situations where a third party company that maintains (rather than owns) data suffers a data security breach (for example, when a data storage facility that stores PII for another business is hacked). In such a case, the actual owner of the information must bear the cost of giving notice under current California law. However, under the California bill that was introduced in 2007 and is still pending, if notice of a data security breach is required, the owner or licensee of the information would be entitled to reimbursement from the third-party entity maintaining the computerized information for "reasonable and actual costs of providing notice to consumers regarding the breach," if the third party-entity that merely holds or maintains the PII suffered or was otherwise responsible for the data security breach. The "reasonable costs" would also include the costs of replacing debit or credit cards in relation to the breach.

Connecticut

Connecticut Senate Bill 1089 would have imposed notice and liability requirements on any person doing business in Connecticut who "owns, licenses or maintains computerized data that includes personal information."[32] The bill's notice provisions would have required that, in the event of a data security breach, all state residents whose personal information may be compromised must be given adequate notice in a reasonably prompt manner. The proposed bill would have imposed liability on any covered person to an FI with customers whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through a breach of security. Liability would include costs incurred by FIs, including the following:

- cancellation or re-issuance of any credit card, debit card or other "account access device";
- closure of any deposit, transaction, or other account as well as other actions to stop payment or block transactions on such an account;
- opening or reopening of any account;
- any refund or credit given to any customer resulting from an unauthorized transaction; and
- any assistance provided to customers to help mitigate loss or inconvenience or to prevent further loss or inconvenience.

Although this measure did not pass, the Connecticut bill would have shifted a significant amount of economic liability from FIs to entities responsible for a data security breach.

Illinois

The state's Credit Card and Debit Card Liability Act,[33] S. 1675, which is currently pending, would amend Illinois law to impose liability on data collectors in the event of a data security breach. The bill would impose liability on the data collector when—

- a credit card or debit card is used to purchase something of value;
- the purchase is made without the consent or authorization of the card's owner; and
- the unauthorized purchase is made as a result of a security breach of the system operated by the data collector, including any breach by an employee or agent of a data collector.

The proposed law would hold the data collector liable to any FI that incurs costs in connection with the unauthorized access to accounts, cards, or funds, including the same costs generally listed under the bill proposed in Connecticut.

Massachusetts

Massachusetts H.R. 213 would impose procedures on "commercial entities" that maintain PII. The bill would add a new chapter entitled "Personal Data Protection," that would have defined the "commercial entities" responsible for providing notice to consumers and/or FIs in the event of a data security breach and would enact liability provisions for those individuals and entities required to give notice under the chapter. The bill would also include additional liability provisions for data security breaches. Any commercial entity required to provide notice to a consumer or an FI would also be liable to any FI for the same costs generally listed under the Connecticut bill. The merchant breach liability provision was not specifically incorporated into a separate omnibus data security bill; therefore it is not likely that the bill will be passed during this session in Massachusetts (although the separate data security breach notice provisions are likely be enacted).

Minnesota

It is important to note that, whereas approximately 38 states have enacted laws mandating notice to consumers of data security breaches, Minnesota recently became the first state to legislatively shift costs associated with data security breaches to the entity responsible for the breach. House File 1758 provides that a person or entity doing business in Minnesota that accepts a credit, debit, or stored value card must not retain or store "card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data" after a transaction has been authorized or, for a PIN debit transaction, beyond 48 hours after the transaction. In addition, the bill requires any person or entity responsible for the breach (or such person's or entity's service provider) to reimburse the FI that issued any affected card for reasonable costs incurred to remedy

the breach (generally, the same costs as those detailed in the Connecticut bill). In addition to reimbursement of costs, the bill gives an FI injured by a violation of the bill's provisions a private right of action against the person or entity responsible for the violation.[34]

New Jersey

The New Jersey measure, A. 4413, would prohibit the state's retailers from retaining transaction authorization data (other than name, account number, and expiration date) from a debit or credit card for longer than the amount of time needed to process the transaction. In addition, the measure would make businesses and government agencies that give notice of a data security breach under New Jersey law liable for resulting costs incurred by FIs (generally, the same costs as those listed in the Connecticut bill). The New Jersey bill is still pending.

Texas

House Bill 3222 would have provided that a business that collects, stores, or maintains "sensitive personal information" must abide by generally all the PCI DSS requirements.[35] In addition, an FI would have been given a statutory right to, under certain circumstances, bring claims against a business involved in a data security breach if that business did not comply with PCI DSS requirements at the time of the breach. Under the bill, the FI would have been able to recover all costs generally listed under the Connecticut bill discussed above. The Texas legislature failed to enact H.B. 3222 before the end of the legislative session.

Conclusion

The outcome of the various cases filed regarding the TJX security breach is uncertain. It is also not clear if other states will follow Minnesota's lead in statutorily shifting liability and costs of identity theft to the entities responsible for data breaches. There has been some discussion of a federal data security breach notice law, and Rep. Barney Frank (D-Mass.), chairman of the House Financial Services Committee, has commented that there could be some provisions designed to shift liability from financial institutions to retailers.

One thing is for certain: With the increase in losses suffered by FIs resulting from data security breaches and identity theft-based fraud, FIs are attempting to shift those costs to retailers the FIs believe to be the "weak link" in the security of PII and data related to financial transactions. Retailers claim that these costs will be too high for them to bear, and FIs already pass the costs of such losses along to retailers in the form of interchange fees for processing debit and credit card transactions. Caught up in this struggle are credit card associations, which are under pressure to increase fines against retailers to improve PCI DSS compliance but also need retailers to participate in their networks.

These issues set the stage for numerous court battles and legislative lobbying efforts by FIs, credit card associations, and retailers. The next several years, then, could see a dramatic shift in thinking about who bears the losses associated with electronic financial transactions and what level of data security protection should be required. **TFL**

Erin Fonté is an associate with Los Angeles office of Pillsbury Winthrop Shaw Pittman LLP. Her practice includes a variety of corporate matters. She focuses on counseling financial services clients on a variety of issues, including technology issues, rights to financial privacy, protection of customer data, and compliance with data security regulations. She can be reached at erin.fonte@pillsburylaw.com. *The author wishes to thank Seth Eaton, a third-year law student at Pepperdine University School at Law, for his research assistance on this article.*

Endnotes

[1]*Most Americans Worry About Identity Theft, According to Poll*, GOVERNMENT TECHNOLOGY, April 5, 2007, available at www.govtech.net.

[2]It should be noted that the 2003 statistics came from a Federal Trade Commission study, and the 2006 statistics came from Gartner's own study, hence there are different statistical methodologies.

[3]Privacy Rights Clearinghouse, *Summary of Recent Surveys and Studies from Javelin Strategy & Research, Better Business Bureau, Identity Theft Resource Center, Federal Trade Commission, Gartner, and Privacy & American Business*, last updated June 2007, available at www.privacyrights.org/ar/idtheftsurveys.htm.

[4]This article refers to the theft or security breach of an individual's "personal financial information," but the reader should be aware that definitions of what type of information gives rise to privacy rights and data security breach rights and responsibilities varies under federal and state laws. Use of PII in this article generally refers to a person's name, mailing address, telephone number, bank/FI account information, or other information that may allow a fraudster to commit identity theft.

[5]Frank W. Abagnale, STEALING YOUR LIFE at 4 (Broadway Books, 2007).

[6]Complaint at 3, *Mace v. TJX Cos. Inc.*, No. 1:07 Civ. 10162 (D. Mass. filed Jan. 29, 2007).

[7]CNN Money, *Lawsuits Mount Over Massive Data Breach at TJX Cos*, June 7, 2007, available at money.cnn.com/news.

[8]CRM Buyer, *Retailers Failing to Meet Customer Data Security Standard*, June 13, 2007, available at crmbuyer.com.

[9]*See* n. 5 *supra* at 3–4.

[10]Associated Content, March 3, 2007, available at www.associatedcontent.com.

[11]Joanne McNabb, Chief, California Office of Privacy Protection, "Identity Theft: Innovative Solutions for an Evolving Problem," Testimony Before the U.S. Senate, Committee on the Judiciary, March 21, 2007, available at judiciary.senate.gov.

[12]On July 5, 2007, the Government Accountability Office released a study that concluded that, of the 24 largest data breaches reported between December 1999 and June 2005, stolen information was used in only four instances to create new accounts or to make fraudulent purchases. How-

ever, the report concludes that the full extent of identity theft from large-scale data breaches is unknown. *See* BNA: Privacy Law Watch, *GAO Says ID Theft-Data Breach Link Limited; Backs Risk Threshold for Federal Notice Law*, July 6, 2007, available at pubs.bna.com.

[13]Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999).

[14]The Financial Privacy Rule is codified at 15 U.S.C. § 6801 through § 6809.

[15]The GLBA uses separate terminology, "non-public personal information," but for analysis under this article, this term is essentially the same as PII.

[16]The Safeguards Rule is also codified at 15 U.S.C. § 6801 through § 6809.

[17]Pretexting provisions are codified at 15 U.S.C. § 6821 through § 6827.

[18]The Electronic Funds Transfer Act is codified at 15 U.S.C. 1601 *et seq*.

[19]The Fair Credit Billing Act is codified at 15 U.S.C. 1601 *et seq*.

[20]Marc L. Songhi, *Retailers Fume Over PCI Security Rules*, COMPUTERWORLD, June 7, 2007, available at computerworld.com.

[21]*Guin v. Brazos Higher Educ. Serv.*, 2006 WL 288483, at 1–2 (D. Minn. 2006).

[22]*Id*. at 13.

[23]BNA: Privacy Law Watch, *Data Security: Contract Claim Against Card Processor Dismissed in BJ's Club Data Breach Case*, June 28, 2006, available at pubs.bna.com.

[24]*Sovereign Bank v. BJ's Wholesale Club Inc.*, No. 1: CV-05-1150 (C.D. Pa. filed June 16, 2006), at 5–6.

[25]*Mace v. TJX Companies Inc*.

[26]Donald G. Aplin, *Data Breaches: Class Claim Alleges TJX Negligently Failed to Adhere to Credit Card Security Standard*, BNA: Privacy Law Watch, Jan. 21, 2007, available at pubs.bna.com.

[27]Complaint at 2, *AmeriFirst Bank v. TJX Companies Inc.*, No. 1:07 Civ. 10169-JLT (D. Mass. filed Jan. 29, 2007).

[28]According to Regulation Y, the following activities are declared to be financial in nature:

> (A) Lending, exchanging, transferring, investing for others, or safeguarding money or securities.
>
> (B) Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death. …
>
> (C) Providing financial, investment, or economic advisory services. …
>
> (D) Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly.
>
> (E) Underwriting, dealing in, or making a market in securities.
>
> (F) Engaging in any activity that the Board has determined, by order or regulation that is in effect on November 12, 1999, to be so closely related to banking or managing or controlling banks as to be proper incident thereto. … 12 U.S.C. § 1843(k)(4).

[29]*Am. Bar Ass'n v. Fed. Trade Comm'n*, 430 F.3d 457 (D.C. Cir. 2005), holding that the regular activities of lawyers and law firms do not fall within the definition of "financial services" under the GLBA.

[30]Complaint at 2, *Massachusetts Bankers Ass'n v. TJX Cos. Inc.*, No. 1:07 Civ. 10162-WGY (D. Mass. filed April 25, 2007).

[31]A.B. 779, 2007–2008, Reg. Sess. (Cal. 2007) (as amended May 14, 2007).

[32]S.B. 1089, Gen. Assem., Jan. Sess., § 1(b) (Conn. 2007).

[33]S.B. 1675, 95th Gen. Assem., Reg. Sess., § 3.01 (Ill. 2007).

[34]H.F. 1758, 85th Leg., Reg. Sess., (Minn. 2007).

[35]H.B. 3222, 80th Leg., Reg. Sess., § 1 (Tex. 2007).