

The Professional Liability Implications of Data Breaches

Submitted By: Kevin M. Gatzlaff**
Doctoral Candidate in Risk Management/Insurance
College of Business
Florida State University
Tallahassee, FL 32306-1110
Phone: 850-443-2026
Fax: 850-644-4077
Email: kmg04k@fsu.edu

Kathleen A. McCullough, PhD
Associate Professor and State Farm Insurance Professor in
Risk Management/Insurance
College of Business
Florida State University
Tallahassee, FL 32306-1110
Phone: 850-644-8358
Fax: 850-644-4077
Email: kmccullough@cob.fsu.edu

**Designated Contact Author

Abstract

In February of 2005, thieves successfully established accounts at ChoicePoint, a major data broker, for the purpose of stealing personal information with which to commit fraud. Subsequently, several major data breach events occurred, fueling concern over privacy and identity theft. States responded with regulations mandating disclosure of data breach events to affected consumers. This paper reviews the history of some significant data breach events, details the costs to individuals and firms resulting from data breaches, describes legislation that states have enacted, and explores the professional liability implications for firms that experience a data breach, including recommendations for preventing their occurrence and mitigating their negative impact. We note that, to this point, courts have been reluctant to award noneconomic damages to customers affected by data breaches. We also note that firms wishing to address data breach concerns with insurance must utilize specialized coverages, as these events are normally excluded from standard coverage forms.

Introduction

In February 2005, ChoicePoint, self-described as the “nation’s leading provider of identification and credential verification services” (ChoicePoint, 2006), disclosed that thieves had created false accounts for the purpose of obtaining personal information with which to commit identity theft and subsequent fraud. Initially, ChoicePoint estimated that the information of 140,000 people had been compromised, and at the time of the announcement, more than 700 documented instances of identity theft had already been directly linked to the data breach (Weber, 2005).

Several circumstances regarding the ChoicePoint data breach combined to produce the watershed nature of this event. First, the sheer magnitude of the breach was alarming. Second, the audacity and purpose of the thieves was disconcerting. Finally, the breach occurred at a data broker, a firm entrusted with storing large amounts of detailed personal information. The sum of these three factors produced a significant reaction as many different entities began to be aware of the potentially massive exposure resulting from data breaches. The ChoicePoint incident heightened previously existing consumer fears about data security and attracted significant regulatory attention, which imposes additional costs on firms that store personal data of customers and employees. It inspired policymakers, consumers, and companies to pay more attention to the risks involved with potential identity theft. Perhaps most significantly, it also raised the specter of liability for firms experiencing a breach of customers’ and/or employees’ personal data.

Unfortunately, the ChoicePoint event was not an isolated instance. An article in *Best's Review* asserts that "(e)very day brings a new story about identity theft" (Green, 2007). The Privacy Rights Clearinghouse has been involved in tracking reports of data breaches at U.S. universities, governmental agencies, and corporations since the ChoicePoint incident in February 2005. Their estimate of the number of records that have been exposed in data breaches at these institutions exceeds 218 million (Privacy Rights Clearinghouse, 2008). This number reveals that the reach of identity theft is potentially both very wide and very deep. The growing incidence of identity theft reports highlights the risks surrounding data breaches and calls for a thorough examination of the issues raised by their occurrence. The goal of this paper is to outline the risks posed to firms by data breaches, to explore the extent to which states have begun to regulate responses to data breach incidents, and to more fully examine the steps a firm can take to protect against threats to firm value posed by data breaches.

The remainder of the paper is organized as follows. First, in Section 1, some examples of data breach circumstances will be described, to illustrate both the depth and breadth of possible data breach incidents. An overview of the costs imposed by data breaches will be presented, and an outline of how professional liability exposure can result from data breaches will be discussed. Next, in Section 2, a discussion of specific state notification requirements pertaining to data breaches will be undertaken. Section 3 will then provide some information about insurance coverage options that firms may have to mitigate the potential for losses due to data breaches. Finally, Section 4 contains advice for firms on

how to reduce the possibility of liability exposure from data breach events, and Section 5 concludes.

Section 1--Description of Data Breaches

Types of Data Breaches

Not all breaches are created equal. Some, like the ChoicePoint incident, involve the deliberate intention of stealing personal information for the purpose of committing fraud. Polo Ralph Lauren, shortly after the February 2005 ChoicePoint incident, suffered a similar data breach wherein hackers obtained approximately 180,000 records containing personal information to be used in future fraud attempts. Criminal responsibility would later be placed on a group based in Eastern Europe, who also would be found responsible for the largest data breach event to date involving TJ Maxx (TechWeb, 2007).

Most data breaches, however, are not as audacious as the ChoicePoint or TJ Maxx incidents. Some data breaches result from the misplacing of computers and data tapes, where the potential for exposure exists but uncertainty over the possibility is present. In June 2005, one of the largest examples of this type of potential breach occurred. One box in a shipment of backup tapes containing personal information on 3.9 million customers of CitiFinancial was lost by the carrier en route to its destination. Similar occurrences happened at Time Warner, involving the data of 600,000 customers, and at Bank of

America, involving the personal data of 1.2 million federal employees (USA Today, 2005).

The consequences of other types of data breaches are often ambiguous. Some instances have involved the theft of computers or backup materials. In late October 2006, a thief stole computers from Gymboree's corporate headquarters. The intent of the thief is unknown, but the computers contained unencrypted human resource information and other personal information on the company's 20,000 employees. Similarly, an employee at CS STARS, L.L.C. (a Marsh affiliate) noticed that a computer was missing in May 2006. Stored on the computer was data belonging to the New York Special Funds Conservation Committee, which included information about workers' compensation recipients. Approximately 540,000 people were affected and notified as a result of the breach (Hofmann, 2007).

Still other data breaches do not fit any of these categories. As an example, in early 2006, the Boston Globe accidentally distributed the personal information of about 240,000 subscribers, including credit and debit card numbers, on the reverse side of paper used in wrapping bundles of newspapers for delivery (Reuters, 2006). Another similar example of an unclassifiable exposure of personal information concerns H&R Block, who in January of 2006 sent out a mailing in which the recipients' Social Security numbers were printed on the mailing label, for anyone to see (Zeller, 2006).

The worst known data theft incident to date occurred in late March 2007, when the computer systems of retailer TJ Maxx were revealed to have been systematically infiltrated over a period of multiple years, and 45 million records of customers who had made purchases were compromised (Greenemeier, 2007). In the relatively short period of time between the ChoicePoint incident and the present, the perceived risk of identity theft from data breaches has gone from slight to ubiquitous.

Costs Imposed by Data Breaches

Even though the circumstances surrounding some of the data breaches may be mundane, the degree of exposure and associated costs for the affected firm can be as substantial as those for more widely publicized events. In the CS STARS instance, though the firm later discovered that no unauthorized access to data occurred, it still incurred not only the unquantifiable costs due to damage to its reputation, but also the costs of notifying the approximately 540,000 individuals whose data was involved (Hofmann, 2007).

Data breaches involving Social Security numbers can potentially expose individuals to financial fraud, particularly credit card fraud. Individuals are protected by law from fraudulent charges in excess of \$50 in these instances, and some credit card companies will waive even this amount, but data breaches and subsequent identity theft can expose an individual to significant personal costs even if immunity from direct financial harm is guaranteed. Re-establishing creditworthiness and repairing damage to one's credit is a time-consuming endeavor. On the high end, the Identity Theft Resource Center in San

Diego estimates that the average individual affected by identity theft spends \$800 and 175 hours to repair the damage (Krause, 2006). The Federal Trade Commission conducted a telephone survey of 136 individuals, concluding that the median amount spent by individuals to repair their credit was \$40, and for these individuals, the median amount of time spent to rectify the situation was 10 hours (Federal Trade Commission, 2007). These two wildly diverging estimates can be reconciled by recognizing that a relatively small number of individuals is impacted extraordinarily, thus skewing the average upward.

Regardless of the average costs, individuals understandably expect to recover their costs from the responsible party. In the TJ Maxx case, a class-action lawsuit was quickly filed on behalf of the affected customers. In September 2007, TJ Maxx offered a proposed settlement consisting of a choice between a \$30 voucher or a \$15 check to customers to compensate them for their lost time in dealing with the consequences of the breach. In addition, as part of the proposed settlement, TJ Maxx has agreed to pay the expense of credit monitoring for three years and several years of identity theft insurance for about 455,000 customers (Kerber, 2007a).

Costs imposed on third parties as a result of data breaches are not limited to individual consumers. In the TJ Maxx case, banks issued a large number of replacement cards to the affected customers. The banks were involved in a class-action lawsuit in an attempt to recover the costs of canceling and reissuing those cards. The lawsuit was settled in December 2007, with TJ Maxx agreeing to pay up to \$40.9 million, including part of the

banks' legal expenses (Kerber, 2007b). Unfortunately for TJ Maxx, the lawsuits do not end there. The company also faces a shareholder lawsuit seeking access to internal documents about the breach, which TJ Maxx has refused to provide (McCarthy, 2007). In all, TJ Maxx estimated the cost of the data breach incident at \$256 million (Kerber, 2007a). Given these very real costs of identity theft from data breaches, the question of liability for firms failing to adequately protect sensitive data becomes pertinent.

Liability Exposure as a Result of Data Breaches

There is ample precedent for firms to be concerned with costs resulting from failure to adequately protect sensitive customer and/or employee data. In early 2006, ChoicePoint agreed to pay a \$10 million fine, the largest ever levied by the Federal Trade Commission, as a result of its data breach. ChoicePoint also agreed to contribute \$5 million to a fund to compensate affected individuals (Vijayan, 2006). Since that incident, the Federal Trade Commission (FTC) has made its position quite clear: it considers failure to maintain adequate data security safeguards an unfair trade practice under Section 5 of the Federal Trade Commission Act of 1914. Since 2002, the FTC has commenced enforcement actions nine times as a result of data breaches, each time requiring both general and specific data security improvements (Schwartz and Janger, 2007). While aimed at improving customer data security, these steps have imposed direct costs on businesses in the form of increased operational expenses. More significantly, they also have raised awareness of an emerging potential professional liability exposure for firms that use or store customer/employee personal data.

This liability exposure is perhaps clarified in cases where the FTC has required certain specific actions in its settlement agreement. For example, in a case of theft of data at BJ's Wholesale Club, the FTC settlement required that a specific person or persons be appointed "to coordinate and be accountable for the information security program" (Federal Trade Commission, 2007). If a future data breach occurs, it is possible that this provision of the settlement agreement could create a future professional liability exposure. Similarly, in the TJ Maxx case, the retailer named one of its executives "Chief Privacy Officer" and established a new position of "Privacy Director" in December 2007 (Kerber, 2007c). This action could trigger a professional liability exposure in the event of future threats to privacy.

Legal Activity Resulting From Data Breaches

Legal activity arising out of the occurrence of data breaches is a relatively new occurrence. As such, there are only a few early indications of how courts have begun to apply tort law to instances of data breaches. In general, there are two primary obstacles that portend difficulty in succeeding in collecting on a liability lawsuit against a firm that has experienced a data breach. First, few jurisdictions have included an explicit private right of action in their data security statutes. Of the 34 states that had notification statutes in place in January of 2007, only three had made explicit provisions for a private right of action (Schwartz and Janger, 2007). As for federal legislation, neither the Gramm-Leach-Bliley Act nor the Health Insurance Portability and Accountability Act provide for a private right of action (Schwartz and Janger, 2007). Consequently, to date there have

been relatively few lawsuits in which individual consumers have attempted to recover costs imposed as a result of data breaches.

Factors Impacting Recovery in Data Breach Cases

Recovery from the perpetrator of the identity theft appears to be rare. The Public Research Interest Group in Michigan conducted a law enforcement survey in 2004, which revealed that less than 10 percent of identity theft cases are solved (Owens, 2004). Consequently, although still rare, it appears more common for customers whose personal information has been stolen to seek recovery from the firm experiencing the breach. To date, customers whose personal information has been exposed (but not yet fraudulently used) have not been successful in their class action lawsuits against responsible firms, primarily because of the difficulty in establishing individual damages.

The Supreme Court has ruled that the named plaintiff in a class action lawsuit “must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class...” (*Simon v Eastern Kentucky Welfare Rights Organization*, 426 U.S.26, 40 n. 20 (1976)). To this point, this ruling appears to have helped shield companies from significant damages awards over data breaches. In *Bell v. Acxiom*, a data broker was sued for failing to adequately protect data. The case was dismissed, due to an inability of the claimant to show that identity theft actually resulted from the breach. Consequently, the failure to show damages limited Acxiom’s liability exposure. Similarly, in *Key v DSW*, the retailer admitted that 96,000 customers

were potentially exposed to identity theft. DSW prevailed in the lawsuit for the same reason; namely, that the damages sustained were insufficient to support a class-action lawsuit (Krause, 2006b). Some have argued that additional damages arising from emotional distress over the potential of identity theft should be recoverable, as in fear-of-disease cases resulting from negligent exposure to toxic substances or infectious disease. To this point, courts have been reluctant to apply this doctrine to identity theft cases (Johnson, 2006).

The first case in the nation to establish an employer's responsibility to protect sensitive data that could be used for identity theft took place in Michigan in early 2005. *Bell v. Michigan Council 25 AFCSME* illustrates the concern that firms might experience over potential liability exposure as a result of data breaches. A union official took a laptop containing names and social security numbers of members home. A jury found that the official's daughter had stolen the information and used it to commit identity theft against 13 union members. Despite the union's contention that it could not be held legally responsible for the acts of unrelated third parties, the jury found that the union was responsible for failure to protect this sensitive data, and returned a verdict in the amount of \$275,000 against the union. The verdict was later appealed and upheld. In this particular case, Michigan law required the existence of a "special relationship" between employer and employee that would lead to a higher expectation of security. That relationship would most likely not exist for many instances of recorded data breaches, and is again specific to Michigan state law (Gordon, 2005).

Recent Developments in Data Breach Cases and Related Costs

However, the environment is changing. As the number of states legislating requirements with regard to data security increases, those responsible for data security at private firms, governments, and universities have an ever-greater responsibility to ensure that their organizations comply with those laws. As the number and stringency of disclosure requirements increases, the number of reported breaches is sure to increase as well. As the number of events continue, and the number of people who are touched by data breaches continues to increase, the courts will likely begin to reassess earlier decisions about the extent of legal liability that can be imposed on a firm experiencing a data breach.

Even though individuals are unlikely to recover large class action awards as a result of data breaches, the costs from the event can still be substantial and deserve consideration. The primary factor limiting the liability of organizations experiencing a data breach is the fact that individual damages are difficult to quantify, and are usually relatively small. Taken in the aggregate, however, the amounts can be staggering. Actual financial damages to individuals resulting from data breaches are normally small because financial institutions cannot hold individuals responsible for the actions of others using their identities fraudulently. Consequently, anticipated damages would generally be limited to lost wages, credit monitoring services, and identity theft insurance for the affected individuals. Different estimates exist as to the cost per affected customer of a data breach. The settlement offered by TJ Maxx was a choice between a \$15 check and a \$30

voucher, good for redemption at one of their stores (Kerber, 2007a). Other independent estimates of the per-record cost of a data breach range between \$15 to \$95 (Krause, 2006a). These costs include security upgrades, loss of productivity, and fines and other penalties, in addition to actual reimbursement costs for affected customers. The variety of the sources of costs resulting from a data breach imply that special coverage is necessary to utilize insurance to manage the risks of a data breach.

Section 2--Disclosure Requirements

Even if liability for damages is avoided, one aspect contributing to the costs incurred by a firm suffering a data breach is the cost of notification. Disclosure requirements aggressively implemented by states in the wake of the ChoicePoint incident further increase the risk of liability for firms involved in data breaches, in addition to mandating certain notification costs. Most of these laws used California's Security Breach Information Act as a model, which states that "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" (California Civil Code, 1798.81.5 and Johnson, 2006). This law, the first in the nation, explicitly defined the duty of a private business to safeguard certain personal information. As of the end of 2007, 39 states had enacted legislation pertaining to mandatory disclosure of data breaches (National Conference of State Legislatures, 2008).

All of these laws impose a duty to notify affected individuals when a data breach occurs, although the “trigger” for notification can differ. In general, there are two different levels that states can adopt signifying when affected individuals must be notified. The first is present in the California statute, and it requires sending notification letters when there is a reasonable likelihood that an unauthorized person has “acquired” personal data (Schwartz and Janger, 2007). The second is present in a federal guideline for notifications regarding breaches at financial institutions. Customers are to be notified when there is a reasonable likelihood of “misuse” of personal information. If the information is simply exposed but does not meet this trigger, only the financial institution’s supervisory regulatory agency is notified (Schwartz and Janger, 2007). Arguments in favor of the latter approach typically warn of consumers being inundated with notices if the California trigger is adopted. Conversely, those who prefer the California trigger note that the delay between exposure of personal information and its misuse may compound difficulties for affected individuals if the less restrictive trigger is adopted.

Of the 34 states¹ that had implemented data breach notification legislation prior to the end of January 2007, twenty-three followed the “acquisition” disclosure trigger in the California statute. Only seven states have adopted the higher standard, requiring a reasonable likelihood of misuse of information must exist before the disclosure responsibility becomes incumbent upon the firm at which the breach occurred. Several states also provide that notification is not necessary if an official investigation concludes that there is no reasonable likelihood of misuse of personal information (Schwartz and

¹ Between the end of January 2007 and the end of the year, 5 states implemented data breach notification legislation. Consequently, at the end of 2007, 39 states had legislation in place.

Janger, 2007). Some states' legislation also provides for the consumer option of a "security freeze". In 25 states, consumers have the right to forbid new credit from being taken out in their name without their express written approval.

Section 3--Insurance Coverage Options and Availability

Firms that opt to try to insure against the varied losses that can occur as a result of a data breach are still in the minority, and coverage options for the different exposures that arise from data breaches continue to evolve. *Best's Review* quotes a principal with Integro as saying that the forms, coverages, and players are "changing every day". The article further describes the situation as "dynamic" (Green, 2007). One employee with Progressive Casualty Insurance was quoted as saying that the most common question asked by banks is if their current coverage included identity theft incidents (Esola, 2007).

Typically, four types of firms commonly seek coverage for losses resulting from a data breach: health care companies, financial institutions, technology companies, and retailers. These types of companies have the highest degree of exposure to losses resulting from data breaches. In the case of health care companies and financial institutions, they fall under the jurisdiction of some federal laws that broach the topic of data security (Schwartz and Janger, 2007).

In general, standardized insurance forms exclude losses arising from data breaches. Additionally, the coverages that are currently offered in the marketplace are not standard. For example, some policies would cover the loss of data and losses from its exposure due to improper destruction (“dumpster diving”), while others would not. Similarly, the treatment of data from stolen laptops is inconsistent across policies (Kaiser, 2007). These “off-the-shelf” coverages rarely fit a company’s needs perfectly. Consequently, coverage must be tailored to each institution’s needs in accordance with the exposure it faces (Guzman, 2008).

Any firm that is exposed to the risk of a data breach and the potential misuse of its customers’ and/or employees’ personal information should consider insurance coverage to mitigate against the potential for loss. Differing characteristics of firms require coverage to be tailored specifically to the firm, but for certain types of institutions, the coverage applications are more straightforward. For example, under Title V of the Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act, or GLBA), the boards of directors of financial institutions have a specific responsibility to protect customer data. The legislation gave authority to the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Federal Savings and Loan Insurance Corporation, and other bank regulatory agencies the authority to create regulations regarding data security. These agencies have issued two such “Interagency Guidelines”, requiring reasonable data security and a response program to handle data breaches (Schwartz and Janger, 2007). However, since directors’ and officers’ liability insurance products frequently include a “failure to maintain” clause, a data breach at a financial

institution likely would not be covered by a directors' and officers' (D&O) policy if the breach were caused by the failure to protect the sensitive customer information (Green, 2007). The more appropriate source for coverage is one of the developing products on the market.

For medical providers and other health care companies falling under jurisdiction of the Health Information Portability and Accountability Act (HIPAA), a responsibility to protect sensitive information is included in the legislation. Failure to adhere to this responsibility might be covered by the firm's errors and omissions coverage, but courts have found that this coverage does not extend to back-office employees, since they do not meet the definition of "medical professionals" (Green, 2007). Further, errors and omissions (E&O) policies at health care providers are primarily intended for medical malpractice, and contain information technology exclusions (Guzman, 2008). Consequently, additional coverage must be sought if a firm wishes to more fully indemnify itself from financial liability in the event of a data breach.

Technology firms have a unique exposure to data breach losses. They might appropriately seek coverage to protect against losses from data breaches with a technology E&O policy with a cyber risk privacy policy added by endorsement. The E&O policy covers failures to perform on a promise, but typically excludes security breach incidents, which is why a cyber risk privacy policy may be a valuable endorsement. A retailer might be better served with a stand-alone "cyber risk" privacy

policy, which covers liability resulting from unauthorized access by outsiders or insiders, the latter of which has historically been the more common occurrence (Guzman, 2008).

Some firms have turned to coverage specifically tailored to cyber-related risks. A cyber risk privacy policy typically covers liability resulting from intentional thefts of personal information, which extends to incidents involving stolen hardware where the intent of the thief is unknown. Although companies offer a variety of coverages, the cost of a regulatory investigation resulting from a data breach is typically covered. Costs of civil action and settlement also are generally covered. Any judgment awarded related to a covered exposure also would be covered, though the majority of cases are settled.

Notification costs can usually be covered by endorsement to the cyber risk policy, although the limit of this specific coverage will generally be lower than the policy limits. Endorsements to the policy also can be added to cover first party losses, such as loss of use. For example, a technology company's website may be hacked and inaccessible, resulting in loss of revenue. Coverage to reimburse the costs of re-creating data can also be added by endorsement (Guzman, 2008).

Section 4--The Minimization of Data Breach Risk

Though the costs to a firm of a data breach can be great, and the risk widespread, there is still reticence to purchase additional coverage to completely shield firms from financial liability in the event of a data breach. Part of this reticence can be attributed to lack of

knowledge about coverages, an underestimation of the firm's exposure to the risk of a data breach, and objections to the cost of a relatively narrow coverage (Kaiser, 2007). Given this reluctance, it is important to identify other risk management approaches to managing the potential liability exposure from a data breach.

One way to reduce the liability exposure of data breaches is to take steps to ensure that they do not occur in the first place. The Payment Card Industry Security Standards Council, L.L.P., has established standards with regard to hardware and software design, as well as general processing policies and procedures that can enhance security of sensitive information. These standards can be used by banks, merchants, and third party processors to minimize the potential for unauthorized access to sensitive information (Bruno-Britz, 2008). Advisors also recommend making data security a responsibility of a specific person who is expected to know the latest techniques and methods to ensure the highest level of data security (Goddijn, 2007).

Some advisors also recommend limiting the number of people who have access to sensitive data, and ensuring that they are accountable for the security of that data while it is away from the workplace and in their possession (Goddijn, 2007). Finally, consideration of cyber risk insurance is recommended in accordance with the risk the enterprise faces. Substantial variation occurs in current policies, so special care must be taken to ensure that the coverage is appropriate for a given firm (Guzman, 2008).

Section 5--Conclusion

Since the watershed ChoicePoint incident in February 2005, data breaches have become more widespread. Several major events have occurred involving the exposure of sensitive personal information, which potentially could be used for identity theft. States have responded with stringent regulations intended to provide consumers with more information when a data breach occurs and personal data is exposed. The costs of a data breach can include not only notification costs, costs for security upgrades, and costs to re-create data, but also may include civil liability for damages as a result of the data breach. However, to this point, courts have been reluctant to impose liability for noneconomic damages. For firms that are concerned about the liability implications of a data breach, special insurance coverages exist, but generally must be tailored to the individual firm. In sum, firms that collect or store personal information should consider insurance coverage as part of a comprehensive risk management plan aimed at reducing the costs of a potential data breach.

References

Bruno-Britz, 2008, Compliance Gains Momentum; PCI Council and Card Brands Get Tough on Data Security Negligence and Get a Turnaround, *Bank Systems and Technology*, January 1, 2008:12.

ChoicePoint, 2006. Website www.choicepoint.com accessed June 30, 2006.

Esola, Louise, 2007, Banks Consider Identity Theft Cover As Criminals Target Data, *Business Insurance*, February 26, 2007: p. 20.

Federal Trade Commission, 2007. Website <http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf> accessed September 17, 2007.

Goddijn, Inga, 2007, Cyber Risks Often Underinsured, *Business Insurance*, September 1, 2007: p. 24.

Gordon, Philip L., 2005, Michigan Becomes the First State in the Nation to Open the Door to Potential Employer Liability for Workplace Identity Theft, *ASAP*, April 2005, accessed February 27 at <http://www.littler.com/presspublications/index.cfm?event=pubItem&pubItemID=11278&childViewID=249&type=all>

Green, Meg, 2007, New Risks, New Coverages, *Best's Review*, December: 61-64.

Greenemeier, Larry, 2007, TJ Maxx Parent Company Data Theft is the Worst Ever, *Information Week*, accessed online February 26, 2008 at <http://www.informationweek.com/news/showArticle.jhtml?articleID=198701100>

Guzman, Mary, 2008. Personal Interview conducted February 26, 2008.

Hofmann, Mark, 2007, Security Breach Charges Settled, *Business Insurance*, May 7: 4.

Johnson, Vincent R., 2005, Cybersecurity, Identity Theft, and the Limits of Tort Liability, *South Carolina Law Review*, 57: 255-311.

Kaiser, David, 2007, Insurance Options Vary as Much as Cyber Attacks, *Business Insurance*, May 21, 2007: p.24.

Kerber, Ross, 2007, Latest TJX Offer Includes Checks or Vouchers, *The Boston Globe*, October 11, 2007: p. D1.

Kerber, Ross, 2007, TJX Agrees to Reimburse Banks, *The Boston Globe*, December 1, 2007: p.D1.

Kerber, Ross, 2007, TJX Creates Executive Jobs to Deal With Privacy Issues, *The Boston Globe*, December 25, 2007: p.C11

Krause, Jason, 2006, Stolen Lives: Victims of Identity Theft Start Looking for Damages From Companies That Held Their Personal Financial Information, *ABA Journal*, 92:36.

Krause, Jason, 2006, ID Theft is Real, But Winning Damages is Elusive, accessed February 11 at <http://www.abanet.org/journal/ereport/n3id.html>

McCarthy, Caroline, 2007, T.J. Maxx Parent Company Sued in Credit Card Hack Probe, *CNET News.com*, accessed February 26, 2008 at http://netscape.com.com/T.J.-Maxx-parent-company-sued-in-credit-card-hack-probe/2100-7348_3-6169450.html

National Conference of State Legislatures, 2007. Website <http://www.ncsl.org/> accessed August 21, 2007.

Owens, Megan, 2004, Policing Privacy: Michigan Law Enforcement Officers on the Challenges of Tackling Identity Theft, accessed February 27, 2008 at <http://pirgim.org/reports/policingprivacy04.pdf>

Privacy Rights Clearinghouse, 2008. Website www.privacyrights.org accessed January 26, 2008.

Reuters, 2006, Credit Data Breach at Two Newspapers, *The New York Times*, February 1, 2006: Section C p. 3.

Schwartz, Paul M. and Edward J. Janger, 2007. "Notification of Data Security Breaches", *Michigan Law Review*, 105:5, 913-984.

Swartz, Jon, 2005, Tapes with Data on 3.9M Missing, *USA Today*: 1B.

Techweb, 2007, Secret Service Busts Four Fraudsters With Ties to TJ Maxx Attack, accessed February 12, 2008 at <http://www.informationweek.com/security/showArticle.jhtml?articleID=201001100>.

Weber, Harry R., 2005. "ChoicePoint Stock Falls After Breach," *Associated Press Online*, Feb. 22, 2005.

Zeller, Tom Jr., 2006, Waking Up to Recurring ID Nightmares, *The New York Times*, January 9, 2006: Section C, p.3.