



LEGAL EXPOSURES TO THE MAXX

***Insurance for Breaches of Data Privacy and
Information Security***

December 1, 2007

By: Kevin P. Kalinich, J.D.
Co-National Managing Director, Professional Risk Solutions
Aon Corporation
Chicago, Illinois
Kevin.Kalinich@aon.com

Legal Exposures to the Maxx

Insurance Coverage For Data Privacy and Information Security

By Kevin P. Kalinich

I. 2008 Reality

A. Loss or Theft of Sensitive Data

The total number of data breach victims in 2006 exceeded the 100 million mark (100, 453, 058) - one record for roughly every three Americans¹. The severity of data breaches increased in 2007.² Even more so for financial institutions.³ TJX, which operates hundreds of T.J. Maxx and other stores in the United States and the United Kingdom, set the new record for being the victim of the largest data theft ever: 45.7 million credit card numbers.⁴ In federal court filings, plaintiffs in the TJX case allege that the breach may have resulted in stealing more than 94 million cards. The old record was held by CardSystems, which suffered 40 million records compromised in a mid-2005 breach. The actual number of breaches may be much higher. An alarming 78% of IT professionals in the United States claim that their companies have suffered unreported insider-related security breaches.⁵

The danger does not stop at the networked servers, but includes employees', vendors' and contractors' laptop computers, wireless portable digital assistant devices, USB memory sticks, iPods/iPhones and other portable data storage devices. Eighty-one percent of respondents in a recent survey reported that their organizations have experienced one or more lost or missing laptop computers containing sensitive or confidential business information.⁶ The survey also found that nearly 40% of executives believe that their company will be the victim of a successful network risk attack.⁷

The exposures are not limited to the United States. In October 2007, personal, banking information of half of UK's population was lost on disks, which was missing for 3 weeks before being noticed. The data on 25 million individuals and 7.25 million families (all families with children under 16), includes names, addresses, dates of birth, national insurance numbers, and, in some cases, bank account details. Banks in the U.K. could end up spending upwards of \$500 million to deal with the aftermath, based on a conservative estimate of \$20 per account, which is how much it would cost a U.S. bank to close down and reopen a bank account following a data breach, according to Gartner Inc.

Given that over 70% of the market capitalization of Fortune 500 companies is attributed to information assets, data and privacy breaches negatively affect financial statements. More than one-third of a group of senior executives and risk professionals surveyed by the Economist Intelligence Unit for ACE European Group, IBM Corp. and KPMG LLP in 2007 view loss of data as the most commonly cited threat.⁸ This paper will address the complex issues of insurance coverage for liability related to data privacy and information security related to personally identifiable information ("PII"). PII is generally defined as the first name or first initial and last name of an individual in combination with the



individual's (1) Social Security number, (2) driver's license number, (3) state identification number, or (4) financial account, debit, or credit card number in combination with any required security code, access code, or password that would permit access to an individual's account (i.e. mother's maiden name).

B. Financial Impact – \$256 Million to \$1.35 Billion Hit to TJX

There is conflicting data as to the actual cost of data breaches.⁹ Two surveys found that companies that lose PII and other sensitive data incur an average cost of \$5 million to \$14 million per breach incident, with costs ranging as high as \$22 million to 50 million.¹⁰ Total cost estimates include the actual cost of internal investigations, outside legal defense fees, notification and call center costs, public relations and investor relations efforts, discounted services offered, lost employee productivity and the effect of lost customers.¹¹ Lost business now accounts for 65% of total breach costs, compared to 54 percent last year.¹² Based on benchmarking information compiled by Aon to date, we estimate that approximately 80% of data breaches have a total cost of less than \$1 million, 15% cause between \$1 million and \$20 million in losses and 5% result in damages in excess of \$20 million.

BJ's Wholesale Club has a \$16 million reserve to cover the costs related to its breach. Discount Shoe Warehouse ("DSW") has set aside \$6.5 million for this purpose, noting that costs could rise to \$9.5 million. ChoicePoint settled with the FTC for \$15 million. TJX stated that it expects to incur in excess of \$256 million in costs and warned that potential future costs are still undetermined. However, estimates of the potential loss run much higher. The lower end of Forrester Research's estimate yield's a figure of \$1.35 billion for TJX's losses over several years.¹³ According to information from a 2007 AIG Webinar, they have observed loss activity of \$715,000 (wrongful release of PII), \$2,400,000 (theft of PII), \$9,400,000 (wrongful access to PII class action settlement) and \$5,000,000 (theft of credit card PII – policy limits loss).

Privacy breaches forced an online bill-payment company out of business. In April 2007 a network technician working for Bellevue, Washington based Web content management company Verbus failed to set up a firewall properly as part of an online bill-payment system service for hospitals. The mistake exposed patient data from at least a half-dozen hospitals across the country.

This paper will focus on privacy and data breaches for which entities may have potential liability. It will not focus on ID theft/fraud of PII that is perpetrated by friends, relatives and other non-institutional sources.¹⁴ According to one analyst group, more than 90% of identity fraud starts off conventionally, with stolen bank statements, misplaced passwords or similar means.¹⁵ Although consumers are not liable for any fraudulent charges to their credit cards above \$50, it can take considerable effort and expense to repair their credit histories. Victims spend an average of 25 - 175 hours trying to resolve the problems caused by identity theft, and, depending on which study one believes, spend from \$50 to \$2,000 to repair the damage, excluding attorney's fees.¹⁶ So while an estimated \$56.5 billion in total losses last year were due to identity fraud (affecting 4% of Americans), this paper will not address those situations where family or friends perpetrated the PII theft. Rather, this paper will address ID theft due to the negligence or security breach of a commercial entity.



The full economic value of privacy and the costs of losing that privacy have not yet been actuarially or judicially quantified. Risk management techniques are being used to calculate the “hard” costs that victims incur to repair privacy breaches, such as the costs of monitoring credit, hiring attorneys and closing accounts and opening new ones. However, metrics are still being developed for the costs related to less tangible damages, such as mental pain and suffering from invasion of privacy and loss of PII.

C. Scope of Peril

1. Direct

In 1988, there were only 60,000 computers online. As of 2006, there were more than 650 million computers attached to the Internet. Data and business processes are being increasingly digitized and networked. New business models are emerging, old models are morphing, and there is increased pressure on corporations to speedily bring products and services to market. All of this has resulted in a worldwide technology and telecommunications infrastructure vulnerable to negligent, vengeful, greedy, and malicious participants.

Companies with any of the following characteristics should take a detailed look at their data security risk management strategy:

- Collection, aggregation, processing, use, transfer, storage, distribution or destruction of sensitive, confidential or proprietary PII, regarding customers, partners, prospects, business information or employees.
- High degree of dependence on electronic processes or PII.
- Provide services or products to others regarding PII.
- Develop, implement or consult regarding systems that others use to facilitate PII.

Nearly every entity in operation today relies on electronic networks (including the information, data, PII and e-records within computer networks), regardless of whether it operates a transactional Web site. Such entities are judged by Wall Street, shareholders, customers and spheres of influence not only by the quality of their products and services, but also on their ability to deliver consistent and predictable earnings. A critical factor in increasing earnings predictability is adequate management of data exposures, both online and offline. These exposures extend far beyond those specific to a corporate Web site. If an entity uses e-mail, computerized accounting, customer relationship management, enterprise resource planning, electronic procurement, RFID, or stores electronic data, it has data exposures. For example, over 1,000 shoppers’ debit information was “skimmed” (obtained from fraudulently replaced Point of Sale systems) at Stop & Shop.

2. Indirect – Outsourcing, Vendors, Independent Consultants, Etc.

Many of the major breaches that have been revealed haven’t been the fault of the company itself, but were due to outsourced suppliers and vendors in the logistics or supply chain. Some corporate executives mistakenly believe that they have transferred the associated liability. The data owner remains liable for data breaches of its IT vendors and other outsourced service providers vs. its customers, patients, employees, students, etc. While a hold harmless and indemnity agreement with the outsourced provider allows some



protection, such agreement is generally useless with respect to customers. A well crafted Privacy and Security policy should cover such exposures.

For large entities with many vendors, there are a number of complex options to ensure that your partners satisfy privacy and security insurance requirements. Such customized solutions may involve one or more of the following: captives, self-insurance and master programs that guarantee a minimum number of participants to make it cost effective and efficient for the insurer, insured and the vendors.

D. Introduction to Data Security and Privacy Breach Insurance

The price tag on lawsuits against entities in the "chain of breach" could cost a firm millions in defense costs, regardless of whether or not they are found liable. Entities should seek full defense and indemnity coverage for all data breach and privacy perils regardless of the source of liability or security framework. There is a separate and distinct insurer's duty to defend and duty to indemnify. The insurer's duty to defend the insured is broader than the duty to indemnify. The insurer's duty to defend is triggered by the third party's allegations, whereas the insurer's duty to indemnify the insured is based on the established facts of the case and the specific terms of the policy. Given the potential multi-million dollar costs of defense, it may be worthwhile to purchase data breach coverage solely to pay for defense costs, although most entities that purchase have the intent of addressing catastrophic damages under the indemnity coverage part.

This paper will set forth insurance coverage options, including a comparison of specific coverage grants, listing of potential insurance markets, policy benchmarking information, and claims payments and handling concerns. To start, different insurers approach coverage for data breaches and privacy in various ways – ranging from some that cover the exposures uniformly in Network Risk policies (also known as Cyber-Insurance), regardless of the insured's industry, to those insurers that provide different coverage for professional services companies, financial institutions, healthcare, media companies and any other company that has risks and liabilities associated with electronic processes and interactions arising from business activities. In any case, the most comprehensive policies provide customized coverage and terms to meet the unique circumstances of each potential insured.

Many entities are underinsured against data breach risks and they either do not realize it or do not understand the potential impact of such risks. Precedent-setting court decisions in 2003 held that standard general liability and property policies exclude coverage for many "intangible property" related exposures. Insurance Services Office ("ISO") policy form changes in 2004 and insurance carrier exclusions dictate a review of one's existing coverage. Corporate governance initiatives, such as the Sarbanes-Oxley Act of 2002 ("SOX"), Gramm-Leach-Bliley Act ("GLBA"), Health Insurance Portability and Accountability Act ("HIPAA"), 39 state breach notification laws, Payment Card Industry ("PCI") data security standard mandate data risk management. Increasingly, well-informed customers, suppliers, distributors and partners contractually require privacy and data breach insurance.

Elements of insurance coverage for PII breaches may be included in a number of different lines of insurance coverage. The foremost coverage is evolving in Network Risk insurance, also known as Cyber-Liability or Privacy and Security insurance. Network Risk insurance is coverage to address the unique 'e-risk' exposures associated with electronic processes, interactions and digital assets arising



from computer-dependent business activities that may effect an entity's financial statements. A well-constructed Privacy and Security policy will include a comprehensive coverage grant to address online and offline data security breaches and related privacy exposures. Such policies may address first party only risks, third party only liabilities, or both.

First-party insurance policies, which cover the insured's own actual losses and expenses, may provide coverage for business interruption losses arising from the interruption, suspension or degradation of an entity's own computer network, including business income, extra expense and contingent dependent business interruption. For example, an entity with an e-commerce site that generates hourly online sales or technology intermediary whose revenues are tied directly to the functionality of its network may desire this coverage (i.e. e-retailers, payment processors, Web site operators, transportation, utilities and financial institutions). In addition, the value of an entity's digital assets may be protected, such as customer data, proprietary information, trade secrets, order fulfillment and credit card or other sensitive data, PII and e-records. Cyber extortion, cyber terrorism, crisis communication expense and forensic investigative services may also be added by endorsement.

Third-party liability coverage, which protects the insured from actual or potential liability to an outside entity, such as customers, patients and employees, provides damage and defense costs suffered by others due to a failure of the insured's computer network, systems and software applications (i.e. healthcare, educational institutions, financial institutions, e-retailers, payment processors, social networking sites, transportation and utilities). This includes liability caused by transmission of a computer virus, unauthorized access, denial-of-service, disclosure of confidential information and identity theft. Such insurance may also cover content-based injuries such as libel, slander, defamation, copyright, trademark infringement and invasion of privacy from the display of material on an entity's web site or inadvertent email. If an entity provides professional services in connection with networks, then those services may also be covered, such as "xSP's," technology consultants, payment processors, credit card system operators and software developers.

Since liability for data privacy and information security generally falls within the realm of third party coverage, the rest of this paper will mainly address third party insurance.

II. Is There Liability From Data Breaches?

A. TJX Changed The Landscape

Prior to TJX, there was not a legally recognized foundation for launching private lawsuits over data breaches.¹⁷ Except for certain "professionals," such as doctors, lawyers, bankers, and others in a position of extreme confidence, the common law has imposed little legal duty to protect PII.¹⁸ However, a number of recent cases, regulatory actions and statutory initiatives have increased the risks of legal liability.

TJX refers to itself as the leading off-price retailer of apparel and home fashions within the U.S. and globally. TJX operates T.J. Maxx, 763 Marshalls, 271 HomeGoods, 127 A.J. Wright stores, and 35 Bob's Stores in the U.S. TJX also operates 185 Winners and 69 HomeSense stores in Canada, as well as 211 T.K. Maxx stores in Europe. Criminal intrusions into TJX's computer system exposed data on at



least 45.7 million credit-card numbers to potential fraud by hackers. Investigations found that, among other things, TJX failed to upgrade its data-encryption system in time to prevent the credit-card data theft in addition to holding on to its customers' personal information unnecessarily and for too long. TJX is facing investigations by the FTC, state attorney generals and multiple lawsuits from individuals and banks accusing it of failing to safeguard private data and of delaying disclosure of the problem.¹⁹ To date, the TJX scorecard reads as follows:

- Costs to notify customers
- Customer class action settlement of United States, Canada and Puerto Rico litigation could cost up to \$177 million, including 3 years of victim assistance/ID Theft insurance, 3 years of credit monitoring and one or two \$30 store vouchers for a select group
- Only 455,000 out of 45.7 million stolen records eligible for settlement offer (less than 1%)
- U.S. District Judge William Young allowed a case brought by a group of New England (including Massachusetts Bankers Association) and Alabama banks against TJX for “implied negligent misrepresentation” in the data-security breach (First case of its kind allowed to continue: prior to TJX, banks that issue credit cards have been liable for fraud losses, while retailers have not). The court filings noted that fraud losses from Visa cards alone are estimated at between \$68 million and \$83 million.
- Shareholder litigation (i.e. Arkansas Carpenters Pension Fund, which owns 4,500 TJX shares, sued TJX to get records showing how it handled computer problems that exposed customer data).
- November 30, 2007, TJX reached a settlement with Visa and Fifth Third Bancorp to resolve potential claims and other disputes by U.S. Visa issuers. According to a document filed with the Securities and Exchange Commission, the Framingham, Mass.-based retailer has agreed to fund up to a maximum of \$40.9 million pretax in alternative recovery payments.
- Data stolen from TJX has surfaced in a number of places, including Florida, where thieves used it to steal \$8 million in merchandise from Wal-Mart stores.
- Fifth Third Bancorp was fined \$880,000 by Visa for its role in the customer data breach at TJX²⁰
- Mandated IT Security improvements, analysis and monitoring
- According to one Securities and Exchange Commission filing, since December 2006, TJX has been working with the Department of Justice, the Secret Service, and the U.S. Attorney in the Boston office in a criminal investigation. TJX is also supplying information to the California attorney general's office, the Canadian Provincial Privacy Commissioners, and the U.K. Information Commissioner, as well as to the London Metropolitan police and others.
- Continuing defense costs, plus possibly be forced to pay plaintiff's attorney's fees
- Future claims

Significant in the TJX merchant banking cases, Judge William Young ruled that even though TJX and its processing bank, Fifth Third Bank, did not have “direct contact with the issuing banks, TJX and Fifth Third knew that the issuing banks were part of a financial network that relies on members taking appropriate security measures.”

B. Data Breach Disclosure Laws, Payment Card Industry and Plastic Card Security



1. 39 State Data Breach Disclosure Laws

California set in motion a trend toward requiring public notification of security breaches with its Security Breach Information Act (S.B. 1386). The law requires that businesses, universities and government agencies notify affected people (including those potentially affected) when there is evidence that PII has been exposed. To date, 38 additional states have followed suit, with some of the statutes imposing obligations to provide security for personal information and data disposal/destruction. In addition, Federal legislation is pending that could preempt or compliment state law in 2008. Prior to the advent of such disclosure laws, there were likely plenty of data breaches, but entities were reluctant to advise affected parties of the occurrences and faced little retribution for failing to do so. Although these laws do not provide for a private cause of action, they have contributed to increased litigation because more consumers are being informed that their PII has been breached.

STATE DATA BREACH NOTIFICATION LAWS

STATE	TIME TO NOTIFY CONSUMERS OF A BREACH OF PERSONAL INFORMATION	CIVIL OR CRIMINAL PENALTIES FOR FAILURE TO PROMPTLY NOTIFY CUSTOMERS OF BREACH	PRIVATE RIGHT OF ACTION	EXEMPTION FOR ENCRYPTED PERSONAL INFO	EXEMPTION FOR CRIMINAL INVESTIGATIONS OR INFORMATION PUBLICLY AVAILABLE FROM GOVERNMENT ENTITIES	EXEMPTION FOR IMMATERIAL BREACHES
Arizona	Most expedient time possible, without unreasonable delay	•		•	•	
Arkansas	Most expedient time possible, without unreasonable delay	•		•	•	•
California	Most expedient time possible, without unreasonable delay		•	•	•	
Colorado	Most expedient time possible, without unreasonable delay	•		•	•	•
Connecticut	Immediately			•	•	•
Delaware	Immediately, in the most expedient time possible, without unreasonable delay	•	•	•	•	



District of Columbia	Most expedient time possible, without unreasonable delay	•	•	•	
Florida	Without unreasonable delay	•		•	•
Georgia	Most expedient time possible, without unreasonable delay			•	•
Hawaii	Without unreasonable delay	•	•	•	•
Idaho	Most expedient time possible, without unreasonable delay	•		•	•
Illinois	Most expedient time possible, without unreasonable delay		•	•	•
Indiana	Without unreasonable delay			•	•
Kansas	Most expedient time possible, without unreasonable delay	•		•	•
Louisiana	Most expedient time possible, without unreasonable delay		•		•
Maine	As expediently as possible, without unreasonable delay	•		•	•
Maryland	As soon as reasonably practicable	•	•	•	•
Michigan	Without unreasonable delay	•		•	•
Minnesota	Most expedient time possible, without unreasonable delay	•		•	•
Montana	Without unreasonable delay	•		•	•
Nebraska	Without unreasonable delay	•		•	•



Nevada	As soon as possible, without unreasonable delay	•	•*	•	•
New Hampshire	As soon as possible				
New Jersey	Most expedient time possible, without unreasonable delay			•	•
New York	Most expedient time possible, without unreasonable delay	•			
North Carolina	Without unreasonable delay	•	•	•	•
North Dakota	Most expedient time possible, without unreasonable delay			•	•
Ohio	Most expedient time possible, but not later than 45 days	•		•	•
Oklahoma	Most expedient time possible, without unreasonable delay			•	•
Oregon	Most expedient time possible, without unreasonable delay	•		•	•
Pennsylvania	Without unreasonable delay	•		•	•
Rhode Island	Most expedient time possible, without unreasonable delay	•	•	•	•
Tennessee	Most expedient time possible, without unreasonable delay		•	•	•
Texas	As quickly as possible	•			•
Utah	Most expedient time possible, without reasonable delay	•		•	•
Vermont	Most expedient time possible,	•		•	•



	without reasonable delay				
Washington	Most expedient time possible, without reasonable delay		•	•	•
Wisconsin	Within a reasonable time, not to exceed 45 days				•
Wyoming	As soon as possible, in the most expedient time possible and without unreasonable delay	•			•

*The private cause of action is assigned to the data collector whose information was breached against the party responsible for the action

2. Payment Card Industry Data Security Standard

Commencing October 1, 2007, big retailers accepting payment card transactions faced fines from \$5,000 to \$25,000 per month if they do not comply with the PCI data security controls mandated by the major credit card companies. Five major credit card system companies, American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International created an organization to develop and maintain security standards for credit and debit card payments. The Payment Card Industry (“PCI”) Security Standards Council manages the PCI Data Security Standard, which applies to merchants, payment processors, point-of-sale vendors, financial institutions and more than a billion card holders worldwide.²¹

Under the PCI standard, all companies accepting payment cards are required to implement a set of 12 security controls for protecting card holder data. The controls include ones related to access control and authentication, data encryption, and transaction logging. Note, however, PCI standards are not yet available for Point-Of-Sale devices or software.

About 325 Tier 1 merchants, those defined as processing more than 6 million card transactions a year, had until September 30 to implement the controls. However, according to estimates from analyst firm Gartner, a good half of them have not complied yet.

In addition to Visa’s \$880,000 fine against Fifth Third Bancorp mentioned above in connection with the TJX case, Fifth Third also paid fines and compensation totaling \$1.4 million following the loss of data from BJ’s Wholesale Club several years ago, according to court filings. Technically, Visa and Mastercard can’t fine merchants directly, but rather levy penalties on banks the merchants pay to process transactions when customer pay with credit cards.

3. Plastic Card Security Acts



Minnesota passed a new Plastic Card Security Act in 2007, which makes breached entities responsible for reimbursing banks credit unions the costs associated with notifying and reissuing cards after a breach. The law also allows private citizens to bring lawsuits against breached companies.

California almost passed a similar recently until vetoed by Governor Arnold Schwarzenegger, although it would not have provided for a private right of action. The closely watched California data breach bill, The Consumer Data Protection Act, would have required retailers to reimburse data breach-related costs to banks and credit unions.

C. Examples of Other Sources of Liability

The existing legal framework for critical infrastructure protection consists of a hodge-podge of state, federal and foreign laws that are generally aimed at deterring certain types of conduct on computer networks.²² Some of the requirements are industry specific, such as GLBA²³ for the financial services sector and HIPAA²⁴ for the health services sector. Other requirements emanate from laws focused on the protection of personal interests of individual employees and customers, government enforcement actions, common law and entities' own privacy policies.²⁵ These laws, and others not discussed here, impose duties to implement certain policies and protection of PII. The following sources provide a brief sampling:²⁶

1. Violation of an entities' own privacy policies
2. International, federal, state and local regulation
 - a. Federal Trade Commission ("FTC") & similar state laws
 - b. Attorney General actions
 - c. Children's Online Privacy Protection Act²⁷
 - d. CAN-SPAM Act
 - e. GLBA²⁸
 - f. Fair Credit Reporting Act
 - g. Fair and Accurate Credit Transactions Act²⁹
 - h. HIPAA
 - i. Computer Fraud and Abuse Act³⁰
 - j. Federal Privacy Act³¹
 - k. EU Privacy Directive (Canada, Australia, Japan and other countries all have broader protections for consumer data than U.S. in one respect or another)
 - l. SOX Section 404
3. Private causes of action

However, the laws and regulations generally do not set forth specific security measures an entity should implement to avoid legal liability. The Federal Privacy Act allows individuals to sue the government for failure to adequately protect PII, but there is no counterpart applicable to the private sector. Yet, liability has been found for security violations via federal statutes, state statutes, federal regulations, FTC Decisions and Consent Decrees and state attorneys general consent decrees. Other than individual lawsuits, where the amount of damages is typically very



low or none, entities have been held liable in two primary ways: via the FTC and/or through consumer class actions brought by private parties or state attorneys general.

D. FTC Action

The FTC has enforcement and administrative responsibilities under 46 laws, including the FTC Act and Fair Credit Reporting Act. The FTC receives more complaints regarding identity theft than any other issue. In the past two years, the FTC has brought more than a dozen enforcement actions under the theory that an entity's failure to take reasonable measures to protect customers' PII is an unfair trade practice in violation of the FTC Act.³²

For example, in 2006, the FTC settled with CardSystems and its successor, Soldius Networks, doing business as Pay by Touch Solutions, for the 2005 security breach that caused millions of dollars in fraudulent purchases.

In 2005, pursuant to its authority under Section 5 of the FTC Act and the Fair Credit Reporting Act, the FTC brought an action against an Atlanta-based consumer data broker whose data had been compromised. As a data broker, ChoicePoint obtains and sells consumer data to more than 50,000 businesses. The data often include names, Social Security numbers, birth dates, employment information and credit histories. The FTC alleged that ChoicePoint sold data to people who did not have a "permissible purpose to obtain them." According to the FTC, ChoicePoint also violated the FTC Act by making false and misleading statements in its privacy policies.

In 2006, the FTC settled with ChoicePoint for a total of \$15 million, which included \$10 million for civil penalties and \$5 million for consumer redress. The settlement also required ChoicePoint to implement new procedures to ensure that it was providing data only to legitimate businesses for lawful purposes, and it also had to establish and maintain a comprehensive information security program. Finally, ChoicePoint has to submit to third-party audits every other year until 2026. In December 2006, the FTC began mailing claims forms to more than 1,400 consumers involved in this PII debacle.

Prior to 2005, the FTC went after entities under the deceptive trade practices statute. FTC pursued actions against Guess Jeans and Petco after they fell prey to hackers. Eli Lilly became a target several years ago after it accidentally released the email addresses of nearly 700 subscribers to its prozac.com email alert.

Notwithstanding such FTC settlements, CardSystems, ChoicePoint, BJ's Wholesale Club and others that have settled with the FTC still face potential liability in the millions of dollars in private litigation for the losses caused by the breaches.³³

E. Private Actions Other Than TJX

Lawsuits charging negligence must show that accepted standards of performance were not met. However, overall, data breach negligence standards are not fully established and are just now beginning to be tested in court. Furthermore, victims of data breaches have not proven significant damages to date. The trend is clear: consumers, employees, patients, partners, government actors and legislators are all



pushing for greater liability for those responsible for breaches. Entities that deal with consumers' PII should prepare themselves for the prospect of increased regulation and enforcement by the government, as well as private enforcement through consumer class actions.

1. 2007 Cases Other Than TJX

Judges have consistently ruled that mere "allegations of increased risk of future identity theft" are insufficient grounds for claiming damages. In *Pisciotta v. Old National Bancorp*,³⁴ the United States Court of Appeals for the Seventh Circuit recently held that breached customers who only sought damages for future credit monitoring and emotional distress did not suffer a "compensable damage" under Indiana law for negligence and breach of contract actions. The decision echoed similar decisions made by other courts in the past.³⁵

However, punitive damages can be awarded for a grossly negligent breach, such as involving medical information, even if the breach was not intentional or malicious.³⁶

In August, multiple class action lawsuits were filed against Certegy Check Services, a subsidiary of Fidelity National Information Services (it is separate from the better known Fidelity Investments), for its alleged failure to properly protect consumer data, implement adequate data security controls, not detecting or responding to the theft fast enough and for failing to adequately monitor the actions of its employees.³⁷ A senior database administrator at Certegy pleaded guilty on November 28 to stealing about 8.5 million customer records and selling them to data brokers, according to court documents in U.S. District Court in Tampa. Certegy provides a check-authorization to financial institutions and merchants across the globe.

In September, Accenture was sued by the Attorney General for Connecticut, alleging negligence and breach of contract in consulting in connection with data privacy.³⁸ The comptroller's office hired Accenture to create a financial data system, and transferred some of the data to a tape that was taken to Ohio where the company was working on a similar project. The backup tape, containing bank account and purchasing card data, was stolen from the car of a state intern in Ohio.

A case brought by CUNA Mutual Group, which insures credit unions against fraud-related losses, against BJ's Wholesale Club in Massachusetts state court, is also being allowed to continue. CUNA's group of credit unions suffered more than \$5 million in fraud losses.

In *Thyroff v. Nationwide Mutual Insurance Company*, decided by the Court of Appeals of New York, held that electronic records that are stored on a computer and are indistinguishable from printed documents and are subject to a common-law claim of conversion in New York.³⁹

2. Employee PII

One publicly disclosed case involved San Diego-based Ligand Pharmaceuticals Inc. According to the San Diego district attorneys office and the plaintiffs' attorney in the case, a lab assistant found a box with 38 former employees' personnel records. The assistant used the information to acquire at least 75



credit cards and \$100,000 in merchandise, open 20 cellular telephone accounts and rent three apartments. The assistant was subsequently convicted and imprisoned. Fourteen of the former employees filed suit, charging Ligand with negligence. A confidential “significant six-figure” settlement was approved by the court.⁴⁰

Similarly, a group of Michigan employees was awarded \$275,000 for losses when their union neglected to safeguard their Social Security and driver’s license numbers. The verdict against Michigan Council 25 of the American Federation of State, County and Municipal Employees is one of the first in the nation to find that a custodian of employee information has a duty to guard the data with scrupulous care.⁴¹

3. “Reasonable” Protections

A 2006 case involving a stolen laptop containing 550,000 people’s full credit information sheds some light on what “reasonable” protections an entity must provide in order to avoid damages. Stacy Guin had a student loan with Brazos Higher Education Service Corporation. Brazos employed a financial analyst to review its loan portfolio and decide which loans to buy and sell. The financial analyst worked from his house in Maryland, and had files related to as many as 550,000 of these loans on his laptop at home. The analyst’s house was burglarized, and the unencrypted files were stolen. Stacy Guin sued Brazos for breach of contract, breach of fiduciary duty and negligence.

The court granted summary judgment for the defendant mortgage company, finding that it was not negligent and that the victims who lost data could not demonstrate any “damages” as a result of the conduct. The court concluded that the defendant had complied with the statutory provisions of GLBA because it had written security policies, had current risk assessment reports, and had “proper safeguards for its customers’ personal information.”⁴²

The lack of details in security regulations, such as SOX, HIPPA and GLBA have been a deterrent to litigation to date. The security frameworks often used to comply with federal guidelines, ISO 17799, and the Control Objectives for IT and Related Technology from the IT Governance Institute have not yet been sanctioned by court decisions. In fact, there have been lawsuits that have sought to establish a precedent of such security frameworks, but they have been settled out of court.

4. Pre-2007 Cases

On September 22, 2006, AOL members sued AOL LLC, the Internet division of Time Warner Inc., stating that the company violated their privacy by posting their search queries online.⁴³ The lawsuit claims that AOL violated the Electronic Communications Privacy Act,⁴⁴ the California Online Privacy Act of 2003,⁴⁵ the California Consumers Legal Remedies Act,⁴⁶ the California Customer Records Act,⁴⁷ the California False Advertising Law,⁴⁸ the California Unfair Competition Law,⁴⁹ and common law.

A June 2005 class action was filed against CardSystems Solutions on behalf of California card holders and businesses accepting credit card payments, alleging that the Arizona-based credit card processing



company failed to keep consumers' credit card data safe, breaking Visa and MasterCard's "Data Security Standards," which forbid storing certain consumer information.

Courts in other data breach cases in 2006, such as those in *Forbes v. Wells Fargo Bank*⁵⁰, *Bell v. Acxiom Corporation*⁵¹ and *Key v. DSW*,⁵² have dismissed similar litigation based on plaintiffs' lack of ability to demonstrate damages stemming from the theft or loss of their PII.

Finally, prior to the TJX case, merchant data-breach lawsuits have been dismissed because the plaintiff was not considered a direct beneficiary. The Pennsylvania State Employees Credit Union ("PSECU") filed suit against Fifth Third Bank to recover \$100,000 it spent on canceling and reissuing 235,000 Visa credit cards compromised in the security breach at BJ's Wholesale Club. PSECU argued that Fifth Third should have been liable for the costs because it was the bank responsible for processing credit card transactions for BJ's and should have ensured the merchant was complying with Visa's security requirements. Yet the court held that PSECU, as an "incidental beneficiary," has no right to enforce the contract between BJ's and Fifth Third. CUNA Mutual Group, Sovereign Bank and Banknorth NA, among others, have also filed claims related to the BJ's breach. Note that Fifth Third did pay out approximately \$900,000 in fraud-related charges to several credit card issuers.



III. Potential Solutions

A. Contractual Allocation of Risk

Entities often engage third party technology firms to perform services that allow such service providers access to the insured's computer systems or data. In such cases, the subject entity should include a provision in the service contract that specifically states that the service provider shall hold harmless and indemnify the entity for any and all damages, costs and fees in connection with liability from the loss or theft of PII. In addition, the service contract should also include a provision that requires appropriate insurance coverage be purchased by the technology provider. Note that the requested language will vary depending upon the services provided, the data at issue, magnitude of potential liability and other particular circumstances. The following language, with appropriate modifications, may be used in most situations involving the allocation of liability with respect to PII or other confidential data. As discussed in Part IV below, the language of the policy is more important than the "name" of the policy type (i.e. Network Risk, Privacy and Security, Professional Liability, Media, General Liability, Data Breach, etc.):

INSURANCE. Technology Vendor warrants that it will maintain sufficient insurance coverage to enable it to meet its obligations created by this Agreement and by law. Without limiting the foregoing, Technology Vendor will maintain (and shall cause each of its agents, independent contractors and subcontractors performing any services hereunder to maintain) at its sole cost and expense at least the following insurance covering its obligations under this Agreement: . . .

(_) Professional Liability Insurance with a combined single limit of not less than _____ Million Dollars (\$_,000,000) per occurrence. Such insurance shall cover any and all errors, omissions or negligent acts in the delivery of products and services under this Technology Vendor Agreement. Such errors and omissions insurance shall include coverage for claims and losses with respect to network risks (such as data breaches, unauthorized access/use, ID theft, invasion of privacy, damage/loss/theft of data, degradation, downtime, etc.) and intellectual property infringement, such as copyrights, trademarks, service marks and trade dress. The Professional Liability Insurance retroactive coverage date shall be no later than the Effective Date. Technology Vendor shall maintain an extended reporting period providing that claims first made and reported to the insurance company within two (2) years after termination of the Agreement will be deemed to have been made during the policy period.

Technology Vendor shall ensure that (a) the insurance policies listed above contain a waiver of subrogation against _____ and its affiliates, (b) the Professional Liability policy names _____ and its affiliates and assignees as additional insureds, and (c) all policies contain a provision requiring at least thirty (30) days' prior written notice to _____ of any cancellation, modification or non-renewal. Within thirty (30) days following the Effective Date, and upon the renewal date of each policy, Technology Vendor will furnish to _____ certificates of insurance and such other documentation relating to such policies as _____ may reasonably request. In the event that _____



reasonably determines the coverage obtained by Technology Vendor to be less than that required to meet Technology Vendor's obligations created by this Agreement, then Technology Vendor agrees that it shall promptly acquire such coverage and notify _____ in writing that such coverage has been acquired. All insurance must be issued by one or more insurance carriers Best rated A- or better. Technology Vendor's insurance will be deemed primary with respect to all obligations assumed by Technology Vendor under this Agreement.

B. Risk Mitigation

Protecting the security of corporate information and computer systems was once just a technical issue to be addressed by the information technology (“IT”) department. Today, however, as information security has evolved into a legal obligation, responsibility for compliance has been put directly on the shoulders of senior management and, in many cases the board of directors. It is, as we enter 2008, a corporate governance issue.⁵³ An entity must (a) understand its information assets risks, (b) implement data security policies and procedures, (c) assign responsibility, (d) develop a formal plan, (e) determine when there has been an incident, (f) respond appropriately, and (g) consider risk transfer (insurance) options.

We have to shift the emphasis on IT security to a larger discussion about business risk. Why? Because we associate IT security with things that have become a very small subset of a much larger and continually growing circle of information technology risk. We have been trained over time to associate IT security with certain actions -- protecting the perimeter of the data center, for example -- and certain products -- intrusion detection, encryption, firewalls, anti-virus software, etc. -- that are all merely tactical and do not address any of the real strategic issues in protecting people and organizations from threats.

SOX, the Payment Card Industry Data Security Standards, the FTC, security breach notification laws and the ISO/IEC 27001 (formerly ISO 17799) best practices standard are among the emerging forces pushing companies to enact tighter controls to address data security and privacy perils.⁵⁴

C. Protecting Confidential Data Against Breach Risks

A good start is to conduct an enterprise risk assessment of an entity’s data security exposures by examining three related risk management practices – risk identification (including data inventory & prioritization), risk quantification, and risk mitigation. Such assessment must include multiple areas within the entity, including R & D, product development, production, sales, servicing, human resources, legal, information technology, IT Security, finance and audit.

Companies working to improve their data security management - including records and information management best practices - have found that the efforts resulted in fewer incidents of unauthorized computer use and a decline in damages.⁵⁵ Yet, on average, 64 % of entities admit that they have never conducted a data inventory to determine the location of customer or employee information contained in various data stores.⁵⁶



Upon completion of a data security risk assessment, an entity should eliminate and mitigate the exposures identified to the extent feasible. Data security risk mitigation may include physical security measures, documented corporate policies, third party assessments, contractual limitation of liability, employee awareness programs and technological safeguards. Demonstration of such mitigation efforts will be required in order to obtain privacy and data breach insurance and will improve an entity's risk management in the event insurance is not purchased.

Aon can help draft an incident response plan and an identity theft services proposal. An incident response plan, a protection being used at some fortune 500 entities, is intended to be an internal policy that an organization may use to supplement the privacy and/or security policy. The purpose of an identity theft services document is to provide the client an overview of the key terms and conditions contained in the quotations from the credit reporting agencies for ID theft services before or after an incident occurs. Options and cost depend upon the scope of the engagement.

IV. Insurance Solutions

A. How Do Insurance Underwriters Quantify the Risk?

Since it is impossible to create and maintain an impenetrable system, an entity may choose to review and evaluate available insurance options which address data and privacy breach exposures. One may find the pricing of these specialized insurance policies is often inconsistent because underwriters do not have a history of claims data upon which to base their pricing. It is recommended that quotations be obtained from several insurers, as differences in pricing as well as terms and conditions can be dramatic. Some insurance carriers offer policies with combined programs of professional liability and data security and privacy with a shared limit of coverage, while some carriers will offer standalone data security and privacy protection. In addition, some carriers will only write such policies if a major insurance relationship exists with the insured. Some insurers require a network assessment and some are satisfied by a simple conference call between the respective IT security experts representing the carrier and the insured.

Unlike more established lines of business insurance there is not yet a set standard for a good privacy and data security underwriting submission (although there are some emerging baseline requirements often sought by the leading insurers). Presenting your company in the most favorable light requires a bit of effort, pulling together information from various disciplines within your company including risk management, legal (contracts, dispute resolution process and litigation), privacy officer, systems/information technology, IT security, sales and marketing, product development, and human resources. If prudent measures are in place in each of these areas, appropriate processes are implemented to coordinate such efforts and this work is well documented in your underwriting submission, your company may be eligible for significant rate credits as well as higher limits and/or lower self-insured retentions.

So what are data security and privacy breach underwriters looking for? The following are some emerging baseline requirements often sought by the leading insurers,⁵⁷ although the process is not as cumbersome as it was two years ago. In fact, a simplified application and a one hour conference call



between IT Security personnel at the insurer and the insured may be sufficient to satisfy carrier requirements.

1. Financial Stability and Lack of Losses (financial statements and loss runs)
2. Employee training, awareness and monitoring
3. Sales Practices
4. Contract Procedures
5. Dispute Procedures, Escalation and Resolution
6. Formal Management Responsibility and Standards
7. Physical Network Security Safeguard Controls
8. Logical Network Security Controls
9. Change Management Controls
10. Internet Content Controls
11. Disaster Recovery and Business Continuity Planning

While each insurer maintains its own underwriting requirements, companies that collect large volumes of PII, with high availability networks or large Internet footprints - or companies that simply require higher insured limits - will need to prove that the importance of each of these areas is understood and that privacy and security exposures have been sufficiently addressed through the preparation of plans and guidelines, the purchase of appropriate hardware and software tools, and ongoing testing, assessments and audits.

The bottom line: privacy and data security insurance underwriters want to know that the applicant takes data security seriously, that the parties responsible for data and privacy are adequately trained and funded, and that loss prevention practices -- including baseline information security controls -- are built into the company's everyday policies and procedures. This ranges from new employee training through the policies and procedures surrounding the handling of sensitive customer data, contractual limitation of liability, along with the installation of new equipment onto the corporate network, and touches nearly every corporate function. While the insurance coverage applications -- for the better privacy and security programs -- include questions in each of these areas, the more documentation that a company can provide proving that they 'walk the walk' can result in significant premium discounts and broader coverage options.

B. Coverage under Existing Policies

1. CGL and Property Policies

Insureds should review their traditional insurance policies, such as the comprehensive general liability⁵⁸ and property policies, to determine the exact scope of coverage for data breaches. Depending upon a company's business and operations, some insurance coverage may be in place under existing policies. Alternatively, it may be possible to add a privacy and data breach endorsement to such policies. However, changes in 2004 to the Insurance Service Organization ("ISO") forms, as well as two 2003 precedent-setting cases, have rendered those options dangerous.⁵⁹



In *Ward General Insurance Services v. Employers Fire Insurance*⁶⁰, the court held that data is not considered tangible property in the context of a property policy; therefore, a loss of data would not constitute a direct physical loss. However, courts have gone both ways on whether the collection of information falls under the “advertising injury and personal injury” coverage part.⁶¹ Similarly, the court in *AOL v. St. Paul Mercury Insurance Co.*⁶², found that computer data is not tangible property under a general liability policy. Privacy and Security policies can address these exclusions, and fill many of the gaps left behind.

Some insurance carriers offer coverage as an enhancement to the property or general liability coverage for traditional insureds. These products are alternatives to stand-alone products (described below) that are designed for entities that use networks as complementary to their traditional brick-and-mortar operations (i.e. not so-called “technology” entities). The coverage features described below are still applicable to these enhancements.

2. Professional Liability and Media Policies

Errors and Omissions (E & O) policies, also known as Professional Liability, are intended to cover third party economic/financial (non-bodily/property injury) damages from errors, omissions or negligent acts of the service or product provider. Similarly, Media Liability Coverage is a type of errors and omissions liability insurance designed for publishers, broadcasters, and other multi-media related firms. Media policies are typically written to cover a few broad areas, such as defamation, invasion of privacy, infringement of copyright and plagiarism. It is important to recognize that broadly worded E & O and Media policies can address all of the same exposures of a Network Risk policy, including data breach and privacy perils. There should be a specific coverage grant to cover liability for damage or loss of third parties’ data caused in the course of the professional services, including unintentional breach of contract coverage for liability arising out of an insured’s collecting, handling, use, transfer and destruction of PII. Each of the Network Risk coverage features discussed below should be considered as well.

3. Other Insurance Policies

It is also possible that, depending upon the facts of the data breach and the particular wording of the policies, Commercial Crime Policies, Employment Related Practices Policies, Data Processing Policies, Computer Fraud Policies, Advertising or Kidnap and Ransom Policies could respond. For instance, if a hacker claims that confidential information will be distributed on the Internet unless the insured pays some type of extortion fee, some Kidnap and Ransom policies may provide defense and indemnity coverage. In general, however, such policies were not intended to cover privacy and data breaches and there are significant coverage gaps in each.

C. Specific Privacy and Data Loss Liability Coverage

Given the uncertainties of each of the policies set forth above and the recognition that modern data breach perils require a different underwriting focus, insurance companies have developed policies that specifically address the loss or theft of PII and other information assets. Perhaps the most significant



recent development in Network Risk insurance is the expansion of available coverage with respect to third party privacy claims, “data protection perils,” coverage for liability arising out of the failure to protect PII from malicious third parties and negligent insiders.

1. State of the Market

As carriers are gaining experience with loss history and underwriting metrics in this area, competition is increasing. However, benchmarking is difficult to categorize and not particularly valuable because each underwriting situation is based on many different factors, such as revenues, business/operations, loss history, mitigation employed, contractual allocation of liability, value of data, number of separate data records, purpose of data records and use of data records. Coverage features should be the primary consideration in an entity’s selection of coverage. Nevertheless, the following summaries provide some general trends through the first quarter of 2007.

2. Carriers

Insurance carriers have different financial ratings that indicate their ability to pay claims. Since the ratings change from time to time, the ratings are not included here, but can be viewed up-to-date online from several sources. There are 10 - 14 core carriers that will affirmatively include data privacy and information security coverage grants in their particular version of a Network Risk policy: AIG (NetAdvantage and ProTech), Ace (Digital Tech & Pro), Beazley (AFB Media Tech), Darwin (Tech/404), CNA (Enterprise Professional Solutions), Hiscox (Technology, Media and Telecoms), St. Paul Travelers (CyberTech), Arch (WebNet Protection through Digital Risk Managers), Hartford (Failsafe Tera), Zurich (Z-Tec E & O), certain Lloyd’s of London syndicates and Media/Professional Insurance (TechNet Solutions – acquired by Axis). Additional carriers will provide excess capacity for large limit programs. Chubb, St. Paul Travelers and Zurich have created special Network Risk products for financial institutions. There are additional carriers that provide elements of data breach coverage for smaller entities, such as Evanston Insurance Co., Euclid Managers (representing Hudson Insurance Co.), InsureTrust (Technology, Media & Information Errors & Omissions Liability), and Safeonline (representing Ace’s Lloyd’s operation).

3. Capacity and Limits

Multi-layer programs with elements of Network Risk have been written with total limits in excess of \$150 million. Carriers that place primary policies offer limits between \$5 million and \$25 million for the first layer, with an average maximum primary layer limit offered of \$10 million. Some carriers require a lower sub-limit for certain coverage related to data breaches, as noted below by specific coverage feature.

4. Deductibles

The amount of deductible required varies dramatically depending upon the revenues, business/operations, loss history, mitigation measures, contractual allocation of liability, average size of sale, number of separate data records, purpose of data records, value of data records, and other factors. Deductibles for typical programs are possible at \$100,000 to \$500,000, with deductibles of \$1 million to



\$10 million required for large programs. Some underwriters require a separate, higher deductible for class action litigation. In addition, if first party coverage is purchased, it is typically subject to waiting periods of 6 to 12 hours

5. Third Party or First Party Coverage

Approximately half of the carriers provide coverage against third party liability claims exclusively. Since this paper is focused on liability from the loss or theft of PII, it will not include an extensive analysis of the first party coverage grants. The greatest distinction between an Errors & Omissions product and a Network Risk product is that some Network Risk products are designed to provide more than just liability coverage and can respond to economic loss experienced by the insured. Such coverage has been especially relevant to electronic retailers (“e-tailers”), and other companies that derive a significant percentage of revenue from network activities. These policies address gaps in traditional property coverage, providing coverage for destruction of intangible assets such as source/executable code, database records, and other electronic documents, as well as Business Interruption caused by certain network events and the extra expense required to investigate, clean up and recover from a virus or other malicious code infection. However, there have been few or no first party claims paid by any insurer. Ask the insurers how many first party claims have been paid.

A first party coverage grant where claims have been paid and is recommended is Computer Crime Coverage. This endorsement provides reimbursement for the amount of money or securities lost as a result of the intentional and unlawful misappropriation of money or securities from the insured resulting directly from the use of the insured’s computer system by an unauthorized person.

6. Pricing

Overall, rates have decreased significantly from three years ago. Again, the differences in pricing can be so dramatic that benchmarking is virtually worthless. Furthermore, often entities make purchase decisions based on pricing rather than the more important factor of coverage features. While the average premium is \$10,000 to \$25,000 per million dollars of limits, the range of premium is \$5,000 to \$50,000 per million dollars of limits. Most 2007 renewal placements have been placed at rates that held flat, although some good risk accounts enjoyed rate reductions where competition was introduced. Various sources estimate that total premiums written by the entire industry for such coverage are between \$100 million to \$500 million. The total premium growth in the first three quarters of 2007 has outpaced prior years.

7. Claims Handling

The primary reason to purchase insurance is to have a claim paid when a covered loss occurs within the policy terms. Therefore, a potential purchaser should seek references and experiences of others in determining the primary carrier. It is also important to interview the claims handling staff at insurance carriers to determine the expertise and experience in handling the type of complex issues that arise in data security and privacy breach claims.

D. Coverage Features and Exclusions



Given the magnitude of diversity in the electronic world, flexibility is important. Each of the carriers referenced earlier address the following features and exclusions in their own unique manner, usually in the form of a separate module to their Network Risk policy. Accordingly, it is essential to read the policy – specific terms, conditions, limitations and exclusions may apply. A potential purchaser may then request the features that its specific circumstances dictate.

1. Scope of Data Breach/Privacy Violation

While first generation Network Risk policies provided coverage for privacy claims that resulted from specific network events/failures, more recent coverage grants provide a broad-based grant of coverage for privacy claims without many of the historical restrictions on the proximate cause of a breach or wrongful disclosure of information. A customized and carefully crafted definition of the insured's "activities" that could give rise to a data security or privacy breach is critical. Broad "all-risks" coverage is preferred over "specified perils" coverage because it is impossible to predict where the next peril will come from (i.e. wireless, RFID, GPS, "phishing," "pharming," "spoofing," "skimming," pre-texting, "botnets," etc.). Exclusion carvebacks should be requested for unsolicited electronic communications, breach of the entity's privacy policy and coverage for suits by employees (employees can have sensitive data lost or stolen just as easily as customers). In fact, such coverage can be offered to employees as a human resources employee benefit. The policy should specifically state that it covers invasion of privacy and defamation.

2. Data Protection and Data Practice Coverage

The policy should cover all of content, electronic records, system facilitation and services, if services are applicable.

3. On-line and Off-line

The coverage should be provided for both on-line and off-line aggregation, storage, transfer, destruction, distribution and use of data. The majority of losses occur from stolen or lost laptops, storage disks, CD's, "dumpster diving," and other offline mediums, which some base forms exclude from coverage because the definition of covered "Computer Systems" only includes appliances connected to the network.

4. Acts of Employees, Independent Contractors and Outsourced Operations

Data breach security and privacy policies generally exclude coverage for intentional wrongful acts, and some states prohibit such coverage on public policy grounds. However, the most comprehensive policies protect innocent insureds from intentional unauthorized access or other wrongful conduct by "rogue" employees, at least covering allegations of intentional wrongful acts until such conduct is established by a final adjudication. Policies should also provide for coverage and defense of insureds for the acts of independent contractors. Many entities outsource large portions of their data storage and retrieval, which must be addressed accordingly.



5. Regulatory Proceedings

Some carriers have shown a willingness to provide meaningful limits of liability and breadth of coverage to address potential loss associated with an insured's statutory obligations to notify customers, and provide certain required services, in the event of wrongful disclosure of information. Defense costs are available, although there is often a sub-limit (i.e. \$250,000 - \$500,000). Indemnity response is less available and the coverage is only provided to the extent allowable under law (many state laws prohibit coverage for statutory or regulatory fines and penalties as against public policy). Furthermore, such coverage grant is typically subject to the carrier's consent.

6. ID Theft Services/Mitigation Costs

Coverage for costs associated with a data breach is available both pre-incident and post-incident. Coverage should include the costs to satisfy statutory notification, credit reports, credit monitoring, call center services, attorney services and public relations expenses. Pre-incident coverage is fairly cheap (approximately 2 – 5 cents per record), but if the coverage is purchased after a breach, it is significantly more expensive (\$10 to \$20 per person just for credit monitoring services). Carriers may eliminate the deductible requirement, but sub-limit the coverage amount.

In the case of a data breach, an incident occurs when there is a loss or theft of PII, which does not necessarily trigger coverage under a standard Network Risk policy. Yet, there are reporting costs, possible fines and penalties, costs to reassure customers and mitigation costs. Claims may not come in for a year or more, and are likely much less in number than the original number of PII records compromised. Insurers have begun to address this issue by adding a trigger that relates to the loss or theft of PII – usually a trigger equivalent to those under state disclosure laws. However, the carriers generally put time constraints on the term of claims coverage from the breach event.

7. Expanded Crisis Management Coverage

This is basically public relations expense coverage that is generally sub-limited under the base policy. There is an insurance product called “adverse reputational insurance” to cover the potential loss in revenues derived from a specified “negative event,” such as a data or security breach.

8. Fines/Penalties/Damages

A well-negotiated and drafted policy will expand coverage to include compensatory, punitive, consequential and multiple damages, as well as pre- and post-judgment interest.

All Network Risk policies exclude coverage for taxes, fines and penalties. This exclusion should be amended to avoid contradiction to the regulatory proceedings enhancement above. As most state laws prohibit insurance coverage for fines and penalties as against public policy, some carriers address this issue by adding elements of coverage to the extent allowable under applicable law. If relevant, coverage for Payment Card Industry fines should be requested.



9. Geographic Scope

As entities cross borders, whether off-shoring or conducting operations, they need to be aware of privacy laws in each foreign jurisdiction, which are constantly evolving. The policy should provide for universal or worldwide coverage, regardless of where the suit or claim is brought. Some claims in foreign countries arise from allegations that are less than formal litigation (i.e. letter complaint) and the policy should include triggers to provide a coverage response.

10. Acquired Entity Coverage

Mergers and acquisitions raise all of the data breach and privacy issues discussed herein all over again – new networks, systems, employees and procedures. It is typical for most lines of insurance to include acquired entities below a certain percentage of total revenue threshold (i.e. 10%) in coverage, although there may be an additional premium due the insurer. However, some Network Risk policies exclude data breach and privacy coverage for acquired entities without complete due diligence underwriting. The theory is that computer systems security (technical, physical, operational and behavioral) varies significantly and the acquired entity may not be “safe.”

11. Additional Terms and Conditions

There are many other terms to consider that are not unique to Network Risk policies, such as Choice of Counsel, Extended Reporting Period options, insured vs. insured exclusions, additional insured status, application of primary policy clauses, “hammer clause,” and prior acts coverage.

V. CONCLUSION

In the past few years, consumers have filed numerous lawsuits against entities involved in data breaches, including against third parties with whom the aggrieved did not have a direct relationship. Although some cases have settled with payments to plaintiffs, prior to TJX, litigation in this area has not resulted in many large liability verdicts for a number of reasons:

- Since there are no laws providing private rights of action to consumers specifically for a data security breach, consumers must generally rely on state consumer protection, false advertising, implied contract, and fraud laws to bring suit against private entities. Such laws are quite vague and do not provide a framework that is adequate for dealing with data security breaches.
- Data security breaches usually do not cause any significant quantifiable harm to the individuals whose information was compromised. In certain situations, courts have therefore labeled the damages claimed by plaintiffs as “speculative” or “nonexistent” and have dismissed lawsuits because of this defect.
- Determining the link between data breaches and identity theft is challenging because, among other things, identity theft victims often do not know how their personal information was obtained⁶³



- The victims in class actions must suffer similarly to be included in the certified class, which may not be the case with respect to data breaches, where victims may have vastly different damages.
- Breached entities want to avoid any adverse publicity and often settle complaints quickly and quietly under confidential terms.
- Breached entities recognize their liability and settle quickly because they don't want these cases to go to trial and establish case law that is going to set bad precedent.
- Criminals may be aggregating massive amounts of stolen data, waiting for credit-monitoring defenses to lapse to maximize their gains.
- Many companies have commercially reasonable security in place, which helps insulate them from liability.

However, as insurance brokers, we have increasingly seen more data breach damage claims by entities that seek defense and indemnity protection from their insurers. Unfortunately for the purposes of this paper (but fortunately for the breached entity), confidentiality obligations prohibit us from disclosing information regarding such claims unless they have been disclosed through publicly available means.

Data privacy and information security exposures continue to evolve in an unprecedented manner due to the unique aspects of electronic business – 24 x 7 x 365 availability, instantaneous interaction, worldwide distribution, dynamic content, and other evolving characteristics. Court decisions provide conflicting legal precedent and insurers have minimal historical claims event data. Recent case law and legislative initiatives suggest a trend toward greater liability for data breach and privacy perils. Maximum financial statement stability related to critical electronic processes and interactions may be achieved through a proactive, comprehensive mitigation initiative combined with data breach and privacy specific insurance coverage. Otherwise, entities may be left with potentially catastrophic gaps in coverage, which could decimate their bottom line. It is worth the time, expense and effort to analyze whether coverage is adequate and what options are available.

This line of insurance is currently far from standardized. Data breach and privacy provisions reflect a great discrepancy in the breadth of coverage provided to insureds, the issues that underlie coverage are numerous and complex. Whether an entity seeks coverage for itself, to cover customers, patients, students and employees or requires its service providers to certify coverage, understanding the intricacies of data breach and privacy coverage is imperative. Understanding what is available and what a given policy covers can be challenging. Entities should seek a qualified attorney and insurance broker who can provide exposure identification, analysis and coverage comparisons to fit the entity's risk profile.

“But we had locks”

Carol Meyerowitz, CEO, TJX Companies, June 6, 2007



¹ <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

² “U.S. Cost of a Data Breach” study, Ponemon Institute (www.ponemon.com). The average cost of a data-loss incident jumped in 2007 to \$197 per record, up eight percent from 2006’s \$182 average and 43 percent from 2005.

³ Financial services entities customers suffer average breach costs = \$239 per record, compared to \$145 in the retail sector. “U.S. Cost of a Data Breach” study, www.ponemon.com. In addition, fraud police are buckling under mountains of data. Up to 300,000 Suspicious Activity Reports are filed per month in the U.S. and up to 200,000 a year in the U.K., but most of those reports “disappear into the black hole” because law enforcement agencies do not have the resources to investigate each one.

⁴ www.sec.gov. According to the Securities and Exchange Commission filing, since December 2006, TJX has been working with the Department of Justice, the Secret Service, and the U.S. Attorney in the Boston office to in a criminal investigation. TJX is also supplying information to the California attorney general’s office, the Canadian Provincial Privacy Commissioners, and the U.K. Information Commissioner, as well as to the London Metropolitan police and others.

⁵ National Survey on Managing the Insider Threat www.ponemon.org

⁶ “U.S. Survey: Confidential Data at Risk.” www.ponemon.org

⁷ The Cost and Confidence Research Study. www.YouGuv.com.

⁸ “Business Resilience: Ensuring Continuity in a Volatile Environment,” www.aceuropegroup.com.

⁹ The most recent study, by Forrester Research, estimates information security breaches cost anywhere between \$90 to \$305 per lost record (www.forrester.com).

¹⁰ Lost Customer Information: What Does a Data Breach Cost Companies? (www.ponemon.org).

¹¹ “U.S. Survey: Confidential Data at Risk.” The survey found that almost 20% of customers immediately terminated their accounts with vendors that lost their information, and an additional 40% considered termination. “National Survey on Data Security Breach Notification,” www.pgp.com/ponemon.

¹² “U.S. Cost of a Data Breach,” The Ponemon Institute.

¹³ According to Forrester Research Senior Analyst Khalid Kark, who admitted the “realistic minimum estimate” may be lower.

¹⁴ The Federal Trade Commission’s Identity Theft Data Clearinghouse established in compliance with the Federal Identity Theft and Assumption Deterrence Act of 1998, receives a weekly average of over 3,000 calls regarding identity theft.

¹⁵ Javelin Strategy & Research, Pleasanton, California.

¹⁶ Privacy Rights Clearinghouse. www.privacyrights.org

¹⁷ John Soma, professor at the University of Denver College of Law and the executive director of its Privacy Foundation. See also: *Doe v. Dartmouth-Hitchcock Mediacl Center*, No. CIV. 00-100-M (D.N.H. July 19, 2001), *Nexans Wires S.A. v. Sark-USA Inc.*, 319 F.Supp.2d 468 (S.D. N.Y. 2004); But see: *Theofel v. Farey-Jones*, 359 F.3rd 1066 (2004); *Charles Schawb & Co. Inc. v. Carter*, No. 04 C 7071 (N.D. Ill. Sept. 27, 2005)

¹⁸ Bruce E. H. Johnson and Kaustuv M. Das, Data Breach Notice Legislation: New Technologies and New Privacy Duties? 865 PLI/Pat 203, 2006

¹⁹ *Amerifirst Bank v. TJX Companies, Inc.* U.S. District Court for the District of Massachusetts, No. 1:07-cv-10169-JLT (January 29, 2007); *Julie Buckley v. TJX Companies*, U.S. District Court for the District of Massachusetts, No. 1:07-CV-10209-RWZ (February 2007); *Jo Wood and Katie Willoughby v. TJX, Inc. and Fifth Third Bancorp*, U.S. District Court for the Northern District of Alabama (Southern Division), No. CV-07-P-0147-S (January 19, 2007); *Anne Cohen v. TJX Companies, Inc.*, U.S. District Court for the District of Massachusetts, No. 1:07-cv-10280-WGY (February 15, 2007); *Thomas Gaydos v. TJX Companies, Inc.*, U.S. District Court for the District of Massachusetts, No. 1:07-cv-10217-WGY (February 5, 2007); *Paula G. Mace v. TJX Companies, Inc.*, U.S. District Court for the District of Massachusetts, No. 1:07-cv-10162-WGY (January 29, 2007); *Brian Churchman v. The TJX Companies* (Statement of claim filed in Canada); etc.

²⁰ Technically, Visa and Mastercard can’t fine merchants directly, but rather levy penalties on banks the merchants pay to process transactions when customers pay with plastic.



-
- ²¹ PCI Security Standards Council, <https://www.pcisecuritystandards.org/index.htm>
- ²² National Academy of Engineering National Research Council of The National Academies, “Critical Information Infrastructure Protection and the Law: An Overview of Key Issues” (www.national-academies.org)
- ²³ 15 USC, Subchapter I, Sec. 6801-6809. PL 106-102.
- ²⁴ PL 104-191.
- ²⁵ Information Security Law Resources (compilation of laws governing Network Security), available at www.bmck.com/ecommerce/home-security.htm.
- ²⁶ According to the Securities and Exchange Commission filing, since December 2006, TJX has been working with the Department of Justice, the Secret Service, and the U.S. Attorney in the Boston office in a criminal investigation. TJX is also supplying information to the California attorney general’s office, the Canadian Provincial Privacy Commissioners, and the U.K. Information Commissioner, as well as to the London Metropolitan police and others.
- ²⁷ 15 U.S.C. 6501 et seq
- ²⁸ Gramm – Leach-Bliley Act, Public L. 106-102, Sections 501 and 505 (b), 15 U.S.C. Sections 6801, 6805.
- ²⁹ People who follow credit card cases will know that one of the most unpopular pieces of legislation among large corporations is FACTA, which limits what can be printed on a credit card receipt. Unpopular because it has led all sorts of people taking them to court over statutory defaults, such as printing more than five digits of the credit card number, or printing the card’s expiration date. More than 100 class action lawsuits have been filed in 2007 against large corporate retailers, including IKEA, Costco, Victoria’s Secret, Toys “R” Us, and other large chains.
- ³⁰ The CFAA applies to all companies and all computers that are connected to the Internet and provides a civil cause of action for anyone who suffers damage or loss because of a violation of the statute.
- ³¹ For example, a class action lawsuit was filed against the postal service for allegedly selling employee’s personal information to marketing companies. *McDermott v. USPS*, 2:07 CV 01174-JCR
- ³² See www.ftc.gov/opa
- ³³ See Kevin J. Kotch, “Insurance Coverage For Liability Arising From Loss Or Theft Of Sensitive Customer Data Under Existing Insurance Policies,” ABA Insurance Coverage Litigation Seminar, March 1, 2007.
- ³⁴ 2007 WL 2389770 (7th Circuit 2007). <http://www.ca7.uscourts.gov/tmp/680M5MZZ.pdf>
- ³⁵ *Kahle v. Litton Loan Servicing*, 486 F.Supp.2d 705, S.D. Ohio 2007, No. 1: 05CV756, May 17, 2007; *Guin v. Brazos Higher Education Service Corp.*, 2006 WL 288483 (D. Minn. 2006); *Stollenwerk v. Triwest Healthcare Alliance* 2005 WL 2465906 (D. Ariz. Sept. 6, 2005)
- ³⁶ *Randi A.J. v. Long Island Surgi-Center* (N.Y. App. Sept. 25, 2007) (involving breach of medical information)
- ³⁷ *Theodore Barreson v. William Sullivan, et. Al.* 2:07 CV 05309 (August 2007)
- ³⁸ *State of Connecticut v. Accenture*, CV-07-5013293 (Conn. Sept. 4, 2007)
- ³⁹ 864 N.E.2d 1272 (N.Y. Ct. App. March 22, 2007)
- ⁴⁰ Dan Bacalski, attorney with San Diego-based Bacalski, Byrne and Koska.
- ⁴¹ *Bell v. Michigan Council*, 2005 Mich. App. Lexis 353 (Mich. App. February 15, 2005)
- ⁴² *Guin v. Brazos Higher Education Service Corporation*, No. Civ. 05-668 RHK/JSM, Feb. 7, 2006, D. Minn. (Not Reported in F.Supp.2nd)
- ⁴³ <http://www.bermanesq.com/pdf/AOL%20Privacy-Cplt.pdf>.
- ⁴⁴ 18 U.S.C. Section 2702
- ⁴⁵ Cal. Bus. & Prof. Code Section 22575, et. seq.
- ⁴⁶ Cal. Civ. Code Sec. 1750, et. seq.
- ⁴⁷ Cal. Civ. Code Section 1798.80, et. seq.
- ⁴⁸ Cal. Bus. & Prof. Code Sec. 17500, et. seq.
- ⁴⁹ Cal. Bus. & Prof. Code Sec. 17200, et. seq.
- ⁵⁰ *Forbes v. Wells Fargo Bank*, 420 F.Supp.2nd 1018 (D. Minn. March 16, 2006).
- ⁵¹ *Bell v. Acxiom Corporation*, 2006 WL 2850042 (E.D.Ark).
- ⁵² *Key v. DSW*, No. 2:06-cv-459 (S.D. Ohio, Sept. 27, 2006).



⁵³ Thomas J. Smedinghoff, “The New Law of Information Security: What Companies Need to Do Now,” *The Computer & Internet Lawyer*, Vol. 22, No. 11, Nov. 2005, p. 10.

⁵⁴ See also, *Wolfe v. MBNA America Bank* (2007): Where injury foreseeable and preventable, defendant had a duty to third parties to authenticate identity of applicants for credit card.

⁵⁵ www.netdiligence.com

⁵⁶ www.ponemon.org

⁵⁷ www.netdiligence.com

⁵⁸ See Kevin J. Kotch, “Insurance Coverage For Liability Arising From Loss Or Theft Of Sensitive Customer Data Under Existing Insurance Policies,” ABA Insurance Coverage Litigation Seminar, March 1, 2007.

⁵⁹ Donald S. Malecki, “Electronic Data and the CGL – Explosion of the use of electronic data triggers coverage gaps,” May 2005.

⁶⁰ No. G031624, (Cal. Ct. App. 4th Dist., Dec. 17, 2003)

⁶¹ See, e. g., *American States Insurance Co. v. Capital Associates of Jackson County, Inc.*, 392 F.3rd 939, 943 (7th Cir. 2004); *Resource Bankshares Corp. v. St. Paul Mercury Insurance Co.*, 407 F.3rd 631 (4th Cir. 2005).

⁶² 347 F.3rd 89 (4th Cir. 2003)

⁶³ According to a report released in July 2007 by the Government Accountability Office prepared for a congressional committee, only one in eight incidents have actually resulted in clear signs of identity theft. A report released in November 2007 by San Diego, California based risk management firm ID Analytics found similar results.

