



Red Flags, Broken Hearts, & Data Breach Stimulus

Insurance for Breaches of Data Privacy and Information Security

June 2009

Copyright 2009 – Aon Corporation

Kevin P. Kalinich, J. D.

Co-National Managing Director, Professional Risk Solutions

Aon Corporation

Chicago, Illinois

Kevin_Kalinich@ars.aon.com

Table of Contents

I. Emerging Threats in Data Breaches	3
A. Frequency.....	3
B. Severity.....	3
C. Scope.....	4
1. Litigation Developments: Broken Hearts.....	5
2. Regulatory Developments: Red Flags & Breach Stimulus.....	6
II. Emerging Solutions in Privacy and Security Insurance	8
III. Sources of Liability	10
A. Statutory (includes international, federal, state and local regulations).....	10
1. Data Breach Disclosure Laws.....	12
2. FTC Actions.....	12
3. Plastic Card Security Act.....	13
4. Payment Card Industry.....	13
B. Case Law (includes violations of one’s online privacy policy).....	14
IV. Risk Management: “Yes We Can” Address Privacy & Security Exposures ...	18
A. Risk Mitigation.....	18
B. Contractual Allocation of Liability.....	19
C. Information Technology Security.....	20
D. Incident Response Plan.....	21
V. Insurance Solutions	22
A. How Do Insurance Underwriters Quantify the Risk?.....	22
B. Coverage under Existing Policies.....	24
1. CGL and Property Policies.....	24
2. Professional Liability and Media Policies.....	24
3. Other Insurance Policies.....	24
C. Specific Privacy and Data Loss Liability Coverage.....	25
1. State of the Market.....	25
2. Carriers.....	25
3. Capacity and Limits.....	25
4. Deductibles.....	25
5. Third Party or First Party Coverage.....	26
6. Pricing.....	26
7. Claims Handling.....	26
D. Coverage Features and Exclusions.....	26
1. Double Trigger.....	27
2. Scope of Data Breach/Privacy Violation.....	27
3. Media Liability.....	27
4. Online and Offline.....	27
5. Insider Acts Coverage.....	27
6. Employee Complaints.....	28
7. Independent Contractors and Outsourced Third Party Providers.....	28
8. Regulatory Proceedings.....	28
9. ID Theft Services/Mitigation Costs.....	28

10. Expanded Crisis Management Coverage	28
11. Fines/Penalties/Damages	29
12. Geographic Scope	29
13. Acquired Entity Coverage	29
14. Additional Terms and Conditions.....	30
VI. Conclusion.....	31
Notes	33

Personally identifiable information (“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).

I. Emerging Threats in Data Breaches

The statistics show that data breaches are becoming more frequent, more sophisticated and more financially damaging. There has been no end to the list of negative impacts from major data breaches, including consumer, patient and employee class action litigation, credit card cancellation and re-issuance costs, fines and penalties, defense of regulatory investigations, costs of crisis management and forensics investigations, and the inevitable legal fees. The spiraling number of high-visibility data breaches has prompted multiple insurers to offer innovative coverage aimed at helping businesses, public entities, utilities, universities and healthcare providers cope with privacy and security risks.

A. Frequency

285 million records were compromised in 2008.ⁱ 74% resulted from external sources, 67% were aided by significant errors and 87% were considered avoidable through simple or intermediate controls. The majority of the lost data was neither encrypted nor protected by a password.ⁱⁱ An alarming 78% of IT professionals in the United States claim that their companies have suffered unreported insider-related security breaches.ⁱⁱⁱ Despite the increase in frequency and severity, thirty-eight percent of Fortune 500 companies surveyed in a new report fail to acknowledge the threat of a data breach in the Risk Factors section of their SEC 10-K filing.^{iv} Additionally, of the companies that do include the risk of a data breach in their 10-K, 26 percent fail to mention the consequential financial impact while a further 49 percent failed to identify the reputational impact.

B. Severity

The average total cost per 2008 breach incident was \$6,300,000.^v The average cost of a data breach hit \$202 per stolen record in 2008, compared to \$197 in 2007, \$182 in 2006 and \$138 in 2005.^{vi} Increasingly, the biggest cost to companies that suffer data breaches is lost business. Approximately \$139 of the average per-record breach cost – or 69% of the total – was in the form of lost business last year, while other costs declined as companies implemented better incident response plans. A U.S. National Archives and Records Administration study found that 25% of companies experiencing an IT outage of two to six days went bankrupt immediately, with even more following in the longer term.

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 yields a figure of \$1.35 billion for TJX’s losses over several years.^{vii} According to information from an AIU Holdings webinar, the company has 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 – insurance policy limits loss).

Some data is worth more to ID thieves than other information. The following lists the least to most valuable:^{viii}

- Your name
- Your address
- Your phone number
- Your date of birth
- Your mother's maiden name
- Your Social Security number (\$.90 -- \$25/each)
- E-mail addresses (\$30 -- \$40/megabyte) & passwords = \$4/each
- Credit Card number, expiration date & security code (\$.10 - \$25/each + \$3.50 - \$12/each for the cards' three or four digit security code)
- Your bank account numbers (\$10 -- \$1,000/each)

Most businesses are not aware of the many factors that can contribute to the financial impact of a data privacy breach. There are "Privacy Breach Calculators" that provide examples of the items an organization should consider when estimating the potential business impacts of a data privacy breach.^{ix}

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.^x According to one analyst group, more than 90% of identity fraud starts off conventionally, with stolen bank statements, misplaced passwords or similar means.^{xi} 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 the study, spend from \$50 to \$2,000 to repair the damage, excluding attorney's fees.^{xii}

C. Scope

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. Data can be breached in a number of data loss methods: data on the move, accidental exposure, insider theft, subcontractors and hacking. In the large majority of breach cases, it is the lax security practices of a third party that allow an attack. It should not come as a surprise that organizations frequently lack measures to provide visibility and accountability for partner-facing systems.

1. Litigation Developments: Broken Hearts

Heartland Payment Systems, Inc. disclosed in January 2009 that hackers had installed malicious software on its computer network sometime in 2008, potentially allowing the band of high-tech criminals based in Eastern Europe to steal millions of credit and debit card accounts. The Heartland Payment Systems data breach has already cost the card processor \$12.5 million in legal fees, related costs and penalties, including a \$6 million fine from MasterCard. A number of class action suits by consumers and financial institutions impacted by the breach have yet to be heard in the courts. Similarly, RBS WorldPay, which also processes payments, was also taken off the PCI-compliant list in March 2009 after it disclosed a significant data breach.

The fall-out so far includes dozens of lawsuits in federal and district courts, formal inquiries by the SEC, the FTC, the U.S. Department of the Treasury, the Comptroller of the Currency, as well as an investigation by the U.S. Department of Justice, stock price plummet and over 656 U.S. financial institutions impacted.

In May 2009 alone, the following privacy and security cases were filed, settled or data breach notices were sent.

- The FTC settled a case against James B Nutter & Company, a mortgage lender that failed to safeguard consumer information. The FTC has filed data security cases against retailers TJX, CVS Caremark and DSW Shoe Warehouse, and the data brokers ChoicePoint and Reed Elsevier, which operates Lexis Nexis and Seisint, Inc. In February 2009, CVS Caremark agreed to pay \$2.25 million to settle charges that it discarded sensitive information into dumpsters. The FTC, which worked with the Department of Health and Human Services in the case, moved against CVS following news reports that CVS's employees threw into dumpsters such things as pill bottles with patient names and medications, papers with credit card information, and employee applications with Social Security numbers.
- A federal class action was filed against claims pharmacy benefits manager, Express Scripts, which allowed unknown people to gain confidential information of its members. The litigation is in connection with an extortion attempt that threatened to publish the confidential information of millions of Express Scripts members on the Internet, some of which has already been disclosed.

- Four HIV-positive patients whose records were left behind on a Massachusetts train by a Massachusetts General Hospital employee are suing the hospital, contending their privacy was breached.
- Merrick Bank launched a multi-million dollar lawsuit against Savvis, accusing the vendor of erroneously telling it that CardSystems Solutions complied with Visa and MasterCard security regulations less than a year before the payment processor's systems were hacked, compromising millions of credit card accounts.
- Online backup service provider Carbonite sued storage vendor Promise Technology, saying repeated failures of Promise gear have caused "significant data loss" at Carbonite." Interactive Digital Systems, a systems integrator, is also named in the suit.
- A data breach at LexisNexis online information service resulted in thousands of customers potentially losing their identities to scammers. LexisNexis Group notified 32,000 people on May 1 that their information may have been stolen and used in a credit card scam that involved stealing names, birth dates and Social Security numbers to set up fake credit card accounts.

2. Regulatory Developments: Red Flags & Breach Stimulus

The Fair and Accurate Credit Transactions Act ("FACTA"), added sections intended to help protect consumers from identity theft. For those businesses that are "financial institutions" or "creditors" that offer or maintain one or more "covered accounts," the U.S. Federal Trade Commission will commence enforcement of the Red Flag Rules as of August 1, 2009. The Red Flag Rules require many businesses to develop, implement, and administer an Identity Theft Prevention Program that is designed to detect warning signs (or "red flags") of identity theft, as well as prevent and mitigate it. The rule is very broad and is not limited to any particular business sector. Quite the contrary, it is directed to not just financial companies, but also many other types of businesses such as telecommunications, utility, auto, retail and healthcare companies – including hospitals and physician practices (any entity that regularly offers, renews, or continues credit, or any entity involved in the decision to provide credit). The steps for compliance will vary on the size and nature of the business, as well as existing data protection policies, but failure to comply may result in civil monetary penalties.^{xiii}

The American Recovery and Reinvestment Act of 2009 allocates \$20 billion toward efforts to move the country closer to full implementation of electronic health records. Buried in the Act is the Health Information Technology for Economic and Clinical Health ("HITECH") Act, which set forth new federal security breach notification obligations for Covered Entities, Business Associates, vendors of personal health records, and related entities. In May 2009, the Department of Health and Human Services and the Federal Trade Commission each finally issued documents to begin to fill in the details of such obligations including encryption for transmission of health information over the nationwide health information network.

The Massachusetts Offices of Consumer Affairs and Business Regulation recently announced that the effective compliance date of a new monumental security regulation will become effective as of January 1, 2010 (the "Massachusetts Regulation").^{xiv} The Massachusetts Regulation will impact almost every business that stores personal data

of Massachusetts employees and residents (whether or not the company operates in Massachusetts, over the Internet or otherwise) and will require significant security and policy changes for most businesses. The Massachusetts Regulation requires, among other things, the encryption of wireless transmissions of personal information and the encryption of personal information stored on portable devices carrying personal information such as laptops, flash drives and PDAs.

II. Emerging Solutions in Privacy and Security Insurance

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”), 44 state breach notification laws, and 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.

Security and Privacy Liability insurance (also called Cyber Liability or Network Risk) is designed to respond to third party liability and related defense costs, as well as some of the insured’s costs following a breach of the security and/or privacy of data. A number of breaches have resulted in full or partial claims payments in 2008 and 2009. Privacy and Security Insurance can reduce the direct financial impact of a breach, but it will not guard against damage to reputation and the consequential loss in client business and future opportunities that can result.

The price tag on lawsuits against entities in the “chain of breach” in the case examples listed above could cost a firm millions in defense costs, regardless of whether or not they are found liable. 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. Depending upon the circumstances of an entity, it may be prudent to purchase defense only coverage, indemnity only coverage, both or neither. The available coverage parts are as follows:

1st Party Coverage Part		Covers:
Information Asset		Damage to or theft of the insured’s information assets from its computer system.
Business Interruption		Lost income suffered as the result of a system outage or extended downtime due to failure of security.
Cyber Extortion		Extortion threats to commit an intentional computer attack against you.
Crisis Management/ Identity Theft Expenses		Various costs, such as notification, credit monitoring and public relations, resulting from a security/privacy breach.
3rd Party Coverage Part		Covers:
Professional Services Coverage		Acts, errors, or omissions in the course of providing professional services.
Content/Media Liability		Personal and advertising injury and some intellectual property infringement arising out of media content created, produced or disseminated by the insured.
Network Security Liability		Breaches in network security or unauthorized access events
Privacy Liability		Wrongful disclosure of confidential information.

Entities considering this coverage should note that the Information Asset and Business Interruption coverage parts have not been especially relevant to date as there have been few first party claims paid by any insurer and significant hurdles to coverage exist, such as waiting periods of 6-18 hours before coverage applies and difficulty in valuing intangible assets and business interruption costs. There are exceptions, however, and one example is an entity whose primary revenue stream is from network/internet activities, such as online retailers.

The value of Privacy and Security Insurance coverage correlates directly to how well an entity quantifies and qualifies its exposures (discussed in Sections III and IV hereinbelow) and customizes a comprehensive program to address such analysis (discussed in Section V hereinbelow). For example, the massive TJX data breach claim was reportedly denied by TJX's Privacy and Security Insurance carriers due, in part, because adequate Retroactive Date coverage for prior acts was not included. The importance of proper policy wording to ensure mutual expectations are met by the parties, as discussed in detail in Section V below, cannot be overstated.

In another example of misaligned expectations, on March 23, 2009, First Bank filed a breach of contract claim against its insurer, Federal Insurance Company (Chubb).^{xv} The policy at issue is CyberSecurity by Chubb, and is meant to cover, among other things, losses stemming from data security breaches. In late 2007, First Bank had such a loss. The First Bank complaint highlights not only the importance of having specialized insurance coverage for data security breaches, but it also previews some of the defenses an insurer might use in resisting payment when there is a loss stemming from a data security breach. Chubb is attempting to deny the \$5 million claim under the \$10 million limit, \$500K deductible policy, because the breach occurred at First Bank's third party outsourced provider, iWire.

III. Sources of Liability

Under the developing case law, the scope of an entity's duty varies depending upon the particular circumstances faced by that entity. Larger, complex entities with a lot of data that process many PII-related transactions will have a more stringent duty than a smaller, simple entity that processes fewer PII transactions.

A. Statutory (includes international, federal, state and local regulations)

There remains a grey area between regulatory mandates of security and legal liability. With respect to consumer class action lawsuits (see e.g. Heartland Payment Systems, Hannaford, RBS Worldpay and TJX) and third party liability to merchant and issuing credit card banks, there is neither a "strict liability" standard nor "safe harbor" exclusion from liability for those entities in compliance with GLB, HIPAA, SOX, the EU Data Protection Directive or the Payment Card Industry Data Security Standard ("PCI DSS").

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.^{xvi} Some of the requirements are industry specific, such as GLBA^{xvii} for the financial services sector and HIPAA^{xviii} 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.^{xix} These laws, and others not discussed here, impose duties to implement certain policies and protection of PII. The following sources provide a brief sampling:^{xx}

1. Violation of an entities' own privacy policies
2. International, federal, state and local regulation
 - Federal Trade Commission ("FTC") & similar state laws
 - Attorney General actions
 - Children's Online Privacy Protection Act^{xxi}
 - CAN-SPAM Act
 - GLBA^{xxii}
 - Fair Credit Reporting Act
 - Fair and Accurate Credit Transactions Act^{xxiii} (Note the "Red Flag" Rules that became effective January 1, 2008, for certain entities – Section 114 of FACTA, which mandates that any creditor that holds PII (i.e. Banks, Thrifts, Mortgage Lenders, Credit Unions and U.S. Branches of Foreign Banks and Lenders, and other "Creditors," such as utility companies, telecommunications companies, healthcare companies, debt collectors, etc.) must develop and implement an Identity Theft Prevention Program by November 1, 2008. The board of directors must sign off on the written plan, which makes them personally liable to the FTC).
 - HIPAA
 - Computer Fraud and Abuse Act^{xxiv}
 - Federal Privacy Act^{xxv}

- EU Privacy Directive (Canada, Australia, Japan and other countries all have different protections for consumer data than U.S. in one respect or another)
- SOX Section 404
- SEC proposed changes to Regulation S – P to address identity theft of securities industry customers
- Basel II

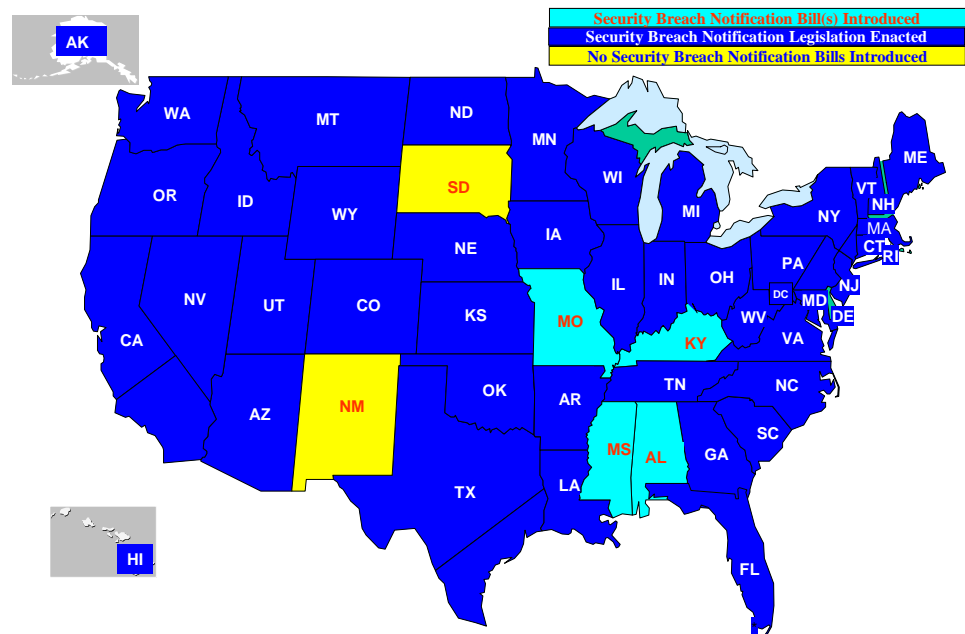
Despite the plethora of oversight, the laws and regulations generally do not set forth specific security measures an entity should implement to avoid legal liability. The Federal Privacy Act allows individuals to sue the government for failure to adequately protect PII, but there is no counterpart applicable 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 litigation brought by credit card issuing banks for the cost of cancelling and reissuing credit cards. Consumer class actions brought by private parties have generally been dismissed or settled due to: A. threat of “Increased Risk of Injury” is insufficient to state a claim; and B. If a private litigant is able to prove “Actual Damages,” each loss is uniquely different that a class action is inappropriate.

There are several actions security professionals should consider to engage product development, treasury, human resources and especially, legal, to communicate their respective concerns, measure legal risks and implement best practices risk management:^{xxvi}

- Legal counsel should be involved in the security compliance process
- Reasonable security is the goal -- not merely technical compliance with security standards
- Consider depth of compliance to ensure the controls in place mitigate the risk to an acceptable level
- Strict compliance reduces legal risk compared to judgment calls involving ambiguities
- Explore use of attorney-client privilege
- Detailed allocation of liability, hold harmless and indemnity in third party vendor contracts

An attorney can understand how a judge, jury or plaintiff's attorney may analyze the entity's security compliance efforts. An assessment of legal risk and implementation of best practices risk mitigation practices could save entities millions if a breach occurs.

1. Data Breach Disclosure Laws^{xxvii}



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, 43 additional states have followed suit, with some of the statutes imposing obligations to provide security for personal information and data disposal/destruction.^{xxviii} In addition, Federal legislation is pending that could preempt or compliment state law in 2009. 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.

2. FTC Actions

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.^{xxix}

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. CardSystems held the old "record" for a data breach prior to TJX – 40 million records.

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 includes 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 mailed 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 (FTC File No. 042 3160) and others that have settled with the FTC still face potential liability in the millions of dollars in private litigation^{xxx} for the losses caused by the breaches.

3. Plastic Card Security Act

Minnesota passed the Plastic Card Security Act in 2007, which makes breached entities responsible for reimbursing banks and credit unions the costs associated with notifying and reissuing cards after a breach. The Minnesota Plastic Card Act is an exception to the generalization as there could be strict liability based on whether an entity is PCI-compliant. The law also allows private citizens to bring lawsuits against breached companies. Additional states are considering similar legislation.

4. Payment Card Industry

Large retailers accepting payment card transactions face 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.^{xxxi}

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, 2007, to implement the controls. In addition to MasterCard's \$6 million fine against Heartland and 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 customers pay with credit cards.

Merchants face a potentially huge liability if they suffer a security breach exposing payment card data. Issuing banks (those that issue credit cards to consumers) have filed lawsuits to recover re-issuance costs allegedly ranging from \$20 - \$50 per card (multiplied by thousands or millions of cards depending on the magnitude of the breach). The potential liability merchants face for payment card security breaches expanded in *Sovereign Bank v. B.J. Wholesale Club & Fifth Third Bank*, No. 06-3392/3405 (3rd Circuit, July 13, 2008). While the Appellate Court affirmed the lower court's dismissal of most of the claims against B.J. Whole Sale Club, it reversed the lower court's dismissal of Sovereign Bank's breach of contract action that was based on a third party beneficiary theory.

B. Case Law (includes violations of one's online privacy policy)

Prior to TJX, there was not a legally recognized foundation for launching private lawsuits over data breaches.^{xxxii} 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.^{xxxiii} However, a number of recent cases, regulatory actions and statutory initiatives have increased the risks of legal liability in some areas and decreased the risk in other areas.

Despite announcing settlements with Visa and MasterCard in 2007, the TJX data security litigation is still going strong in 2009. While most of the credit card issuing banks impacted by the TJX breach are no longer pursuing TJX and/or have settled via Visa and MasterCard dispute resolution processes, two financial institutions, Amerifirst Bank and SELCO Community Credit Union are pressing forward. The U.S. Court of Appeals for the First Circuit allowed three theories of liability to proceed: two claims based on negligent misrepresentation and a third claim previously dismissed alleging that TJX's inadequate security amounted to an unfair business practice under Massachusetts' unfair and deceptive business practices law. Such result is different to that in another Massachusetts' state credit card breach lawsuit (*Cumis Ins. Soc. Inc. v. BJ Wholesale Club, Inc.* 23 Mass. L. Rep. 550 [Mass Super. 2005]) that granted a defendant a motion for summary judgment on the issue of negligent misrepresentation. TJX, which operates hundreds of T.J. Maxx and other stores in the United States and the United Kingdom, set the record for being the victim of the largest data theft ever: 45.7 million credit card numbers.^{xxxiv} In federal court filings, plaintiffs in the TJX case alleged that the breach may have resulted in stealing more than 94 million cards.

A U.S. District Judge on May 12, 2009, became the latest jurist to rule in favor of data-breached retailers, telling Hannaford consumers that because they were compensated by their banks, they have no basis to sue civilly.^{xxxv} All but one of the legal claims filed against Hannaford Bros. – the Maine-based retailer that suffered a security breach exposing some four million credit and debit cards and 1,800 reported cases of fraud – has been dismissed. The company was hit with class-action lawsuits alleging breach of implied contract, breach of implied warranty, negligence and violation of Maine’s Unfair Trade Practices Act. The judge ruled that without actual and substantial loss of money or property, consumers could not seek damages. In the course of coming to its decision, the Court solidified the idea that no legal duty exists to provide “perfect” security – security obligations will be judged on a reasonableness standard instead.

Under Maine law as I understand it, when a merchant is negligent in handling a customer’s electronic payment data and that negligence causes an un-reimbursed fraudulent charge or debit against a customer’s account, the merchant is liable for that loss. In the circumstances of this case, there may be also be liability under Maine’s Unfair Trade Practices Act for an unfair or deceptive trade practice. **But if the merchant is not negligent**, or if the negligence does not produce that completed direct financial loss and instead causes only collateral consequences – for example, the customer’s fear that a fraudulent transaction might happen in the future, the customer’s expenditure of time and effort to protect the account, lost opportunities to earn reward points, or incidental expenses that the customer suffers in restoring the integrity of the previous account relationships – **then the merchant is not liable.**^(ld)

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*,^{xxxvi} the United States Court of Appeals for the Seventh Circuit 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.^{xxxvii}

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.^{xxxviii}

In August 2007, 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.^{xxxix} A senior database administrator at Certegy pleaded guilty on November 28, 2007, 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. On January 9, 2008, Certegy reportedly settled for \$4 million.

In September 2007, Accenture was sued by the Attorney General for Connecticut, alleging negligence and breach of contract in consulting in connection with data

privacy.^{xi} 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, the court held that electronic records that are stored on a computer are indistinguishable from printed documents and are subject to a common-law claim of conversion in New York.^{xli}

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.^{xlii}

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.^{xliii}

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.^{xliv} The lawsuit claims that AOL violated the Electronic Communications Privacy Act,^{xlv} the California Online Privacy Act of 2003,^{xlvi} the California Consumers Legal Remedies Act,^{xlvii} the California Customer Records Act,^{xlviii} the California False Advertising Law,^{xlix} the California Unfair Competition Law,^l 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*^{li}, *Bell v. Acxiom Corporation*^{lii} and *Key v. DSW*,^{liii} 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.

IV. Risk Management: “Yes We Can” Address Privacy & Security Exposures

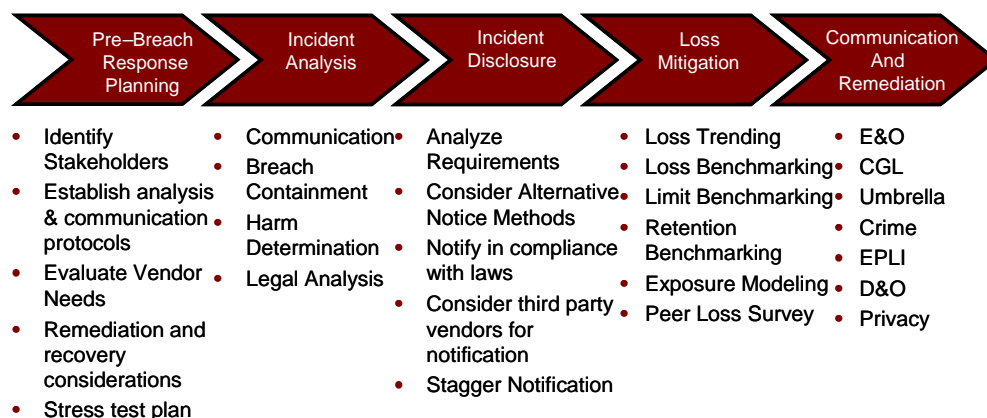
One of the biggest problems we face is when the bean counters -- the CFO's -- [are only] looking at the budget and saying, 'Get the cheapest thing you can so that we can have a checkbox for compliance purposes,' and a checkbox from a compliance initiative standpoint does not necessarily make your company more secure*

A. 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, in 2009, a corporate governance issue.^{iv} 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.

The Five Step Survival Guide

Security Breach Management Framework



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.^{iv}

Heartland was another wake-up call. While the “100 million” number and the “largest breach ever” was speculated by the press, the breach was someone else’s data. Scores of companies suddenly had to enact their data breach incident response plans. Many companies had plans that anticipated vendor initiated breaches – and some did not.

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, 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.”^{vi}

The lack of details in security regulations, such as SOX, HIPAA and GLBA have been a deterrent to litigation to date. The security frameworks often used to comply with federal guidelines, 27001 (formerly 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.

B. Contractual Allocation of Liability

In the PCI related context, entities can reduce their liability by disclaiming all third-party beneficiaries. For instance, merchants can reduce their liability by negotiating a “private safe harbor” in their merchant agreement with their merchant bank/acquiring bank and credit card processors. The goal would be to provide a contractually enforceable safe harbor that would limit liability, fines and penalties from the merchant bank if the merchant is PCI compliant at the time of a breach.

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 V 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, Cyber, 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 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 policy names _____ and its affiliates and assignees as additional insureds, and (c) it will provide 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.

C. Information Technology Security

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.^{lvii} 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.^{lviii}

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.

A skilled insurance broker 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. For instance, a Data Breach Response Plan may include: 1) Harm Determination (Technical Forensics and ID Theft Analytics), 2) Notification and Public Relations (Legal, Campaign and Fulfillment), 3) Credit Reporting Agency (Credit Services, Victim Fraud Assistance and Identity Theft), and 4) Call Center (Preparation and Inbound and Outbound Call Services).^{lix}

D. Incident Response Plan

The value of an incident response plan may be illustrated by the comparison charts below from two actual data breach cases. The primary difference between the two entities is that the entity that prepared and implemented an incident response plan limited its liability and payments to those PII records that actually “opted in” to take advantage of remediation offers. The second entity purchased credit monitoring, breach response, etc. for every possible PII record – even the 85% of PII record holders who did not request it. The pre-litigation breach will be exponentially more expensive than the litigated breach due to the lack of adoption of an incident response plan by the pre-litigation breach entity.

Scenario 1: Costs through Litigation

No Breach Management Plan

A financial services provider discovers a complex virus that had slowly transmitted out nearly **600,000 customer records** over a 2 year period. Once the company went public a class action lawsuit quickly follows alleging that customers were victims of ID Theft. The recently settled incident had the following costs:

Expense Type	Cost
Technical Forensics	\$225,000
Legal Expense	\$15,000
ID Theft Forensics (initial and ongoing)	\$900,000
Mailing costs - 3 complete mailings Includes embedded legal costs as well as primacy and secondary notification to the “class”	\$1,600,000
Call Center (Overflow only. Mostly handled in house)	\$75,000
Public Relations Expense	\$50,000
Credit Monitoring (variable rate per activation)	\$1,900,000
Defense Costs	\$1,100,000
Additional Settlement Costs (including plaintiffs fees, and TPA ID theft claims)	\$3,000,000
Total	\$8,865,000

Scenario 2: Pre-Litigation Costs

Breach Management Plan in Action

A services provider to the entertainment industry suffers a virus attack that leaks data over a 3 year period resulting in over **500,000 lost customer and employee records**. A lawsuit is pending. The incurred losses to date:

Expense Type	Cost
Technical Forensics	\$40,000
Legal Expense	\$5,000
ID Theft Forensics	\$0
Mailing costs 1 mailing	\$1,500,000
Call Center (Outsourced)	\$400,000
Public Relations Expense	\$20,000
Credit Monitoring (blanket purchase @ fixed rate)	\$7,500,000
Defense Costs	\$190,000
Additional Settlement Costs	\$0
Total	\$9,655,000

V. 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,^{ix} although the process is not as cumbersome as it was just 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.

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.

The first step in the underwriting process is the completion of an application and/or self-assessment. It is important that the risk management team engage the appropriate information security and privacy personnel in the application process to provide complete and accurate information. The assessment and application process also provides an opportunity to critically examine an entity's information risk management strategies.

In conjunction with the base application, a potential insured should be prepared to provide the following:

- Copies of privacy policies
- Standard contracts and vendor agreements
- Results of any external or internal audits or assessments that illustrate the information security posture - examples include SAS 70, PCI, or ISO 27799/27001.
- Details of any security breach incidents and the response to them, including any new protocols put in place to prevent similar incidents.
- Financial information
- Customer/Partner/Employee/Patient/Student statistics
- Payment Processing
- Outsourced operations and activities

In addition to an analysis of the standard application materials, underwriters will ask targeted questions in response to the current environment and the latest breach incidents. Recent concerns include outsourced services, data encryption protocols, and wireless access security.

Aon recommends that, as part of a comprehensive risk management strategy, entities work with experienced brokers who are experts in security and privacy coverage and the corresponding legal issues and who have a thorough understanding of the evolving dynamics of both the insured's industry and the insurance marketplace. The underwriting process must be skillfully managed and the complexity of coverage demands innovation and expertise. Those companies who successfully utilize these resources in their risk management process will realize the benefits of this enhanced coverage.

B. Coverage under Existing Policies

1. CGL^{lxi} and Property Policies

Insureds should review their traditional insurance policies, such as the comprehensive general liability^{lxii} 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.^{lxiii}

In *Ward General Insurance Services v. Employers Fire Insurance*^{lxiv}, 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.^{lxv} Similarly, the court in *AOL v. St. Paul Mercury Insurance Co.*^{lxvi}, 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).

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/intangible 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. However, even when clearly intended to be covered, the insured may need to fight the insurer to recover defense and indemnity costs.^{lxvii} 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 Practices Liability 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 2009.

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, Ace, Beazley, BRIT, Darwin (acquired by AWAC), CNA, Hiscox, St. Paul Travelers, Arch, Hartford, Zurich, 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.

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 a median 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 first party claims paid by any insurer.

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 2008 renewal placements were 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 2008 outpaced prior years by over 50%.

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. Double Trigger

A well crafted Privacy and Security policy will have two triggers – one for litigation or threatened litigation against the insured and a second trigger if the insured must comply with any of the data breach disclosure laws.

2. 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. Cloud computing, SaaS, Social Media/Networks, 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.

3. Media Liability

Media liability, which responds to personal and advertising injury claims arising from online or print media and advertising content, is often included in the same policy. This serves a dual purpose of expanding the Advertising Injury (AI)/Personal Injury (PI) coverage in the insured's GL policy and ensuring that data breach-related claims, like invasion of privacy and/or publication of private facts, are covered when they arise from content. One example would be the unintentional publication of a database of patient names and social security numbers on the insured's website.

4. Online and Offline

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.

Early versions of network risk policies were tied to "network security" breaches and were meant to respond to breaches of the insured's computer network security only. Today's network risk coverage responds to breaches of the security and/or privacy of information by online or offline means, arising from electronic devices not connected to a network like laptops, PDAs, data tapes, or external hard drives, or from non-electronic incidents like dumpster diving or the theft of paper files or log books.

5. Insider Acts Coverage

Security and privacy policies generally exclude coverage for intentional wrongful acts, and some states prohibit such coverage on public policy grounds. A broad policy should include a severability provision that maintains coverage for the entity even if the wrongful act was committed maliciously by an employee. Policies should also provide for coverage and defense of insureds facing allegations of intentional wrongful acts until such conduct is established by a final adjudication.

6. Employee Complaints

As with most third party liability policies, there is an insured vs. insured exclusion in all security and privacy policies. The broadest policies now include a carveback to cover the entity for claims made by employees in the event that a breach involves employee information.

7. Independent Contractors and Outsourced Third Party Providers

Many entities outsource functions like billing and data storage to third party vendors, and have a number of third party vendors with access to PII. Policies should respond on a blanket basis whether the breach is caused by an employee of the insured or by an independent contractor or vendor operating on behalf of the insured.

8. 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 U.S. 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.

9. 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. Notice sublimits may apply as well.

10. Expanded Crisis Management Coverage

Coverage is available for a number of the costs that can result from a data breach event. It is important for an entity to clarify its priorities in this area, since the available limit and scope of coverage differs by carrier. Covered costs can include consumer notification, provision of credit monitoring, operation of call centers and related ID theft services or the services of a public relations, law or crisis management firm. Carriers impose a variety of sublimits, different retentions and/or coinsurance provisions to this coverage.

Entities should ask the following questions when considering ID Theft Expense/Crisis Management coverage:

- Is the trigger a reasonable belief that identity theft may occur as a result of a particular incident or is it tied to statutory obligations only?
- Does the policy only pay those costs the insured is required to incur by law or does it provide for voluntary expenses such as providing credit monitoring in a state where the law does not require it?
- Is the insurer's prior written consent required before coverage will apply? Is there a reasonableness standard for consent?
- Are costs incurred solely to mitigate damage to the insured's reputation covered?
- What time constraints apply? Can the insured recover costs under this coverage part more than 1 year after a breach?
- Do the covered expenses mesh with the insured's crisis response plan? Are the insured's preferred crisis management vendors pre-approved?

11. 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 and add back coverage under foreign laws where permitted. 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.

12. 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.

13. 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 system security (technical, physical, operational and behavioral) varies significantly and the acquired entity may not be “safe.”

14. 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, waiver of subrogation, application of primary policy clauses, "hammer clause," and prior acts/Retroactive coverage.

VI. 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 had 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 obtained.^{lxviii}
- 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 increasingly have 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, social media, wireless applications, 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

Notes

- ⁱ 2009 Data Breach Investigations Report, A Study conducted by the Verizon Business RISK Team, www.verizonbusiness.com.
- ⁱⁱ Identity Theft Resource Center, www.ITRC.com, www.databreaches.net, www.datalossdb.org, www.privacyrights.org
- ⁱⁱⁱ National Survey on Managing the Insider Threat www.ponemon.org
- ^{iv} “Data Privacy and Corporate America: Who’s recognizing the risk?” April 2009, www.hiscox.com
- ^v www.ponemon.com
- ^{vi} www.ponemon.com
- ^{vii} According to Forrester Research Senior Analyst Khalid Kark, who admitted the “realistic minimum estimate” may be lower.
- ^{viii} Symantec’s “Underground Economy Report”
- ^{ix} <http://www.informationshield.com/privacybreachcalc.html>
- ^x 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.
- ^{xi} Javelin Strategy & Research, Pleasanton, California.
- ^{xii} Privacy Rights Clearinghouse. www.privacyrights.org
- ^{xiii} www.ftc.gov/redflagrule, “Fighting Fraud With The Red Flag Rule,” A How-to guide for Business
- ^{xiv} 201 CMR 17.00
- ^{xv} First Bank v. Federal Insurance Company, No. 4:09-cv-00532 (Mo. Cir. Ct.) March 23, 2009. See also Ruiz v. Gap, April 4, 2009, California Federal District Court – N.D. CAL, Case No. 07-5739 SC,
- ^{xvi} 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)
- ^{xvii} 15 USC, Subchapter I, Sec. 6801-6809. PL 106-102.
- ^{xviii} PL 104-191.
- ^{xix} Information Security Law Resources (compilation of laws governing Network Security), available at www.bmck.com/e-commerce/home-security.htm.
- ^{xx} 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.
- ^{xxi} 15 U.S.C. 6501 et seq
- ^{xxii} Gramm – Leach-Bliley Act, Public L. 106-102, Sections 501 and 505 (b), 15 U.S.C. Sections 6801, 6805.
- ^{xxiii} 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.
- ^{xxiv} 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.
- ^{xxv} 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
- ^{xxvi} “Who is Minding the Legal Risk around PCI?” Information Systems Security Association Journal, April 2009, David Navetta.
- ^{xxvii} Also see: “Data Breach Notification Law Across the World from California to Australia,” University of New South Wales Faculty of Law Research Series, 2009, Paper 11, Alana Maurushat.
- ^{xxviii} International notification triggers differ from the norm in U.S. States. For instance, the privacy commissioners of Canada, Australia and New Zealand support notification of individuals when there is a risk of harm to them from a privacy breach. A major shortcoming in the U.S. is over-notification.
- ^{xxix} See www.ftc.gov/opa
- ^{xxx} 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.
- ^{xxxi} PCI Security Standards Council, <https://www.pcisecuritystandards.org/index.htm>

-
- ^{xxvii} 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 Medical 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 Schwab & Co. Inc. v. Carter*, No. 04 C 7071 (N.D. Ill. Sept. 27, 2005)
- ^{xxviii} Bruce E. H. Johnson and Kaustuv M. Das, Data Breach Notice Legislation: New Technologies and New Privacy Duties? 865 PLI/Pat 203, 2006
- ^{xxvix} 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.
- ^{xxv} *In Re Hannaford Bros. Co. Customer Data Security Breach Litigation*, MDL Docket No. 2:08-MD-1954, May 12, 2009, D. Brock Hornby, U.S. District Ct.
- ^{xxvi} 2007 WL 2389770 (7th Circuit 2007). <http://www.ca7.uscourts.gov/tmp/680M5MZZ.pdf>
- ^{xxvii} *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)
- ^{xxviii} *Randi A.J. v. Long Island Surgi-Center* (N.Y. App. Sept. 25, 2007) (involving breach of medical information)
- ^{xxix} *Theodore Barreson v. William Sullivan, et. Al.* 2:07 CV 05309 (August 2007)
- ^{xi} *State of Connecticut v. Accenture*, CV-07-5013293 (Conn. Sept. 4, 2007)
- ^{xii} 864 N.E.2d 1272 (N.Y. Ct. App. March 22, 2007)
- ^{xiii} Dan Bacalski, attorney with San Diego-based Bacalski, Byrne and Koska.
- ^{xiiii} *Bell v. Michigan Council*, 2005 Mich. App. Lexis 353 (Mich. App. February 15, 2005)
- ^{xlv} <http://www.bermanesq.com/pdf/AOL%20Privacy-Cplt.pdf>
- ^{xlv} 18 U.S.C. Section 2702
- ^{xlvi} Cal. Bus. & Prof. Code Section 22575, et. seq.
- ^{xlvii} Cal. Civ. Code Sec. 1750, et. seq.
- ^{xlviii} Cal. Civ. Code Section 1798.80, et. seq.
- ^{xlix} Cal. Bus. & Prof. Code Sec. 17500, et. seq.
- ⁱ Cal. Bus. & Prof. Code Sec. 17200, et. seq.
- ⁱⁱ *Forbes v. Wells Fargo Bank*, 420 F.Supp.2nd 1018 (D. Minn. March 16, 2006).
- ⁱⁱⁱ *Bell v. Axiom Corporation*, 2006 WL 2850042 (E.D.Ark).
- ⁱⁱⁱⁱ *Key v. DSW*, No. 2:06-cv-459 (S.D. Ohio, Sept. 27, 2006).
- ^{iv} 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.
- ^{lv} 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.
- ^{lvi} *Guin v. Brazos Higher Education Service Corporation*, No. Civ. 05-668 RHK/JSM, Feb. 7, 2006, D. Minn. (Not Reported in F.Supp.2nd)
- ^{lvii} www.netdiligence.com
- ^{lviii} www.ponemon.org
- ^{lix} ID theft protection services could also be a problem. In February 2008, Lifelock, which touts itself as one of the largest providers of identity theft protection services in the U.S., was sued by Experian for allegedly placing false fraud alerts on consumer credit-history files maintained by Experian as part of its credit reporting business.
- ^{lx} www.netdiligence.com
- ^{lxi} "Insurance Coverage Under Standard Commercial General Liability Policies for Claims Arising Out of Misuse of Personal Data," *The Secure Times*, Spring/Summer 2008, page 10, Stephen Palley.
- ^{lxii} 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.
- ^{lxiii} Donald S. Malecki, "Electronic Data and the CGL – Explosion of the use of electronic data triggers coverage gaps," May 2005.
- ^{lxiv} No. G031624, (Cal. Ct. App. 4th Dist., Dec. 17, 2003)
- ^{lxv} 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).
- ^{lxvi} 347 F.3rd 89 (4th Cir. 2003)

^{lxvii} Ace v. Ascend One Corporation, Amerix Corporation, Civil Action No. CCB-06-3371, U.S. District Court For the District of Maryland, August 7, 2008, Catherine Blake, U.S. District Judge.

^{lxviii} 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.

About the Author

Kevin P. Kalinich co-leads Aon's national practice to identify exposures and develop insurance solutions related to Technology Errors and Omissions, Miscellaneous Professional Liability, Media Liability, Network Risk and Intellectual Property. A 2007, 2008 & 2009 Risk & Insurance "Power Broker," Kevin has been quoted in numerous publications, including the WSJ, Time and Business Insurance Magazine, and a frequent speaker regarding Professional Liability related issues in various venues, including CNBC, RIMS, CRIMS, American Bar Association, American Bankers Association, Defense Research Institute, Society of Risk Management Consultants, Contract Management Association and Stanford University Program in Law, Science and Technology. Joined Aon in September 2000, from Altima Technologies, where he served as Chief Executive Officer and led the successful launch of a Web-enabled software product that provides intelligent visualization of network equipment in the areas of telecommunications, data, cables, and computers. Prior to Altima, was a partner at Chapman and Cutler Law Firm, where he represented domestic and international public and private entities in general corporate matters, intellectual property, M & A, venture capital, institutional investor and IPO transactions. Holds a Juris Doctor from The University of Michigan and received his B.A. degree in Mathematics, Cum Laude, from Yale University.