MAYER·BROWN

Privacy and Data Security in Service Provider Arrangements

Recent Developments

Rebecca S. Eisner

Mayer Brown LLP

June 2009

Professional Profile of Rebecca S. Eisner

Rebecca S. Eisner is a partner in the Chicago office of Mayer Brown LLP. Her practice focuses on complex global and offshore technology and business process outsourcing transactions, including IT infrastructure, applications development and maintenance, back office processing, ERP implementations, finance and accounting, payroll processing, call center, HR, technology development, system integration and hosting. She regularly advises clients in business process services agreements, strategic alliances, joint ventures, licensing, development and telecommunications agreements, and Internet and e-commerce law issues, including data transfer and privacy issues and electronic contracting and signatures. She is a frequent writer and speaker on outsourcing, licensing and e-commerce topics. She is also recognized by *Chambers Global - The World's Leading Lawyers* in the area of Information Technology, and Business Process Outsourcing (2004-2009), Who's Who in American Law, Best Lawyers in America in Information Technology, and Illinois Leading Lawyers. Prior to re-joining Mayer Brown in 1996, Ms. Eisner worked in-house as Associate Group Counsel and Assistant Vice President, Equifax, Inc., Atlanta, from 1993-1995. Her prior work experience also includes serving as a Public Relations and Government Affairs Specialist for The Dow Chemical Company, Midland, Michigan. Ms. Eisner attended the University of Michigan Law School, J.D. (*cum laude)*, 1989, and earned her undergraduate degree in Journalism *(cum laude)* from The Ohio State University.

The author also acknowledges with appreciation the work and research contributed by associates Mark Oram, Joe Pennell and Michael Word, as well as Damoun Delaviz, Swathi Gandhavadi and Ben Williams, who served as summer associates with the firm.

TABLE OF CONTENTS

Page

Page

I. WHY YOUR COMPANY SHOULD CARE ABOUT PRIVACY ISSUES

Privacy issues have been prominent outside of the U.S. for years now.[1] Within the U.S., unless you are in a regulated industry, your company may have given only a passing thought to privacy and data security compliance.[2] However, recent enforcement actions, new laws and class action lawsuits are providing a wake-up call for all businesses handling sensitive customer information (*i.e.*, social security numbers, credit card numbers and other account numbers).[3] Standards for securing private information are emerging, and companies need to take note.

Corporate boards and executives are realizing the effect that security and privacy violations may have on a company. In a 2006 CSI/FBI Survey, 56% of company respondents reported an unauthorized use of their computer systems within the past 12 months.[4] Moreover, several companies have experienced dramatic stock price declines after a major data security breach and privacy violation.[5] As discussed below, several existing laws and regulations require the board or executives to certify as to or approve of security programs. These developments have caused high level groups such as the Business Roundtable and the Corporate Governance Task Force to state that information security requires CEO attention and is a top priority for board review.

Privacy and security are different but are inseparably related. Without the growing body of privacy and data breach laws, security lapses involving private information might have fewer consequences for the company. Without appropriate security measures, protection of private information would be impossible. Privacy of personal information is the result of good security compliance.

Companies have many types of corporate data that they need to protect. Personal information about individuals, whether customers or employees, is just one category, but it is the category with the most recent legal developments.[6] In this category, data breaches and other similar privacy

violations are driving some new legal standards. For example, from 2005 through May 27, 2009, over 261 million records involving sensitive personal information have been involved in security breaches.[7] Breaches like these have spawned some lawsuits and enhanced regulatory scrutiny. Companies need to be aware of the emerging standards created by the legal and regulatory developments, and to determine if their current and planned security and data protection programs comply. No security and privacy program is complete without a compliance and monitoring program for third-party service providers.

With respect to these third parties, outsourcing arrangements often involve the handling of or access to personal information of a business.[8] This is especially true with the burgeoning growth of business process outsourcing, where onshore and offshore providers now handle such services as mortgage loan servicing, benefits and insurance administration, medical records transcription, income tax preparation, help desk functions for product support, billing and payments, and many other functions involving the use, processing or storage of personal information. Privacy compliance and security now belong high on the checklist for every outsourcing transaction.

This article raises important topics that every company should address with its outsourcing service providers (both onshore and offshore). We begin with an overview of the existing privacy legal landscape in the U.S., as well as a look at the emerging U.S. standards applicable to company security and privacy programs. We also examine the emerging standards applicable to third-party service provider arrangements. This article then examines planning for compliance through contractual clauses with service providers, including both onshore and offshore service providers.

II. OVERVIEW OF U.S. PRIVACY LAWS

A. <u>Federal Laws and Federal Regulation</u>. U.S. privacy laws to date exist in targeted industries, such as the financial and medical and health industries. Gramm-Leach-

Bliley ("GLB") and the Fair Credit Reporting Act ("FCRA") are the federal statutes and regulations that regulate the sharing of financial information with third parties and affiliates.[9] For health and medical information, the Health Insurance Portability and Accountability Act and implementing regulations (collectively, "HIPAA") regulates the privacy of health and medical information and the maintenance of electronic health information.[10] The Children's Online Privacy Protection Act of 1998 and regulations (collectively, "COPPA") addresses the collection of personal information from children under the age of 13.[11] The FTC has been active in bringing enforcement actions for violations of COPPA.[12] Outside of laws targeted at government functions,[13] these are the primary general federal privacy laws regulating the use and collection of personal information.

There are several other federal laws that bear on privacy issues in specific industries or contexts. For example, there is the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") regulating the disposal of consumer report information;[14] the Fair Debt Collection Practices Act[15] regulating the manner in which entities may seek to collect debts from consumers; the USA PATRIOT Act[16] regulating anti-money laundering surveillance; and the Right to Financial Privacy Act[17] regulating the disclosure of financial information by a financial institution to the federal government.

Outside of those targeted industries and specific contexts, privacy is largely a self-regulated activity, but an activity to which the Federal Trade Commission ("FTC") has devoted significant attention. The FTC has also devoted a fair amount of resources to enforcement of privacy issues, under the powers granted to the FTC regarding unfair and deceptive business practices. According to FTC Chairman. Jon Leibowitz, "*all* companies must implement reasonable security for and limit their retention of sensitive consumer data. *All* companies must keep their promises about how they will use consumers' information. If they fail to do so –

whether first party or third party, online or offline – we will go after them."[18]

In the earlier days of FTC privacy enforcement, the actions focused on broken promises in privacy statements. More recently, the FTC has changed its focus. Lax security resulting in breaches involving personal information is possibly actionable, even in the absence of a breach incident. As discussed below, this trend of expansion of enforcement will continue.

B. <u>State Laws and State Regulation</u>. The states have also taken notice of privacy and security issues, and have begun enforcement of such issues. Some states have created an agency/office dedicated to this issue.[19] Many states have statutes and regulations that mirror the requirements of GLB and protect personal health information like HIPAA. Several states also have laws regarding the proper disposal of consumer information, use of social security numbers,[20] and other similar protections. The state attorneys general are empowered under state laws regarding unfair business and deceptive practices acts to enforce laws for privacy violations.[21] These powers are similar to those exercised by the FTC under Section 5 of the FTC Act.[22] Additionally many states have passed data breach notification laws and some states are passing data encryption and security program laws. Massachusetts' new data security regulations are the most prominent example of state legislation taking a highly detailed, prescriptive approach to safeguarding personal information.[23] Other states have passed consumer identity theft and health care privacy laws. New York has gone one step further and issued a comprehensive privacy guide for businesses.[24]

III. EMERGING STANDARDS FOR PRIVACY AND SECURITY

Companies that want to implement security measures to protect personal information and other corporate data face a difficult reality: a lack of specific guidance regarding security measures and legal standards. The legal standards from the laws and regulations discussed above provide little

specific guidance. Cases and enforcement actions currently seem to lead to differing standards and technical requirements.[25] Many regulators and legislators are reluctant to mandate specific security measures. Specific measures can quickly become obsolete, or may actually hamper the development of better security technology measures if regulators set the "ceiling" for a security measure. There is some merit in maintaining a higher level, flexible approach that provides room for industry standards to mature and evolve. Even recognized technical information security and general security standards established by industry standard setting groups tend to be high-level. In some cases these technical information security standards are difficult or nearly impossible to achieve in a commercially reasonable manner across all of a company's operations.[26] With the mandate for security and privacy compliance, and the lack of specific guidance, determining the appropriate legal standards and resulting technical measures can seem like navigating without a compass. However, there are some common themes. More importantly, the emerging standard may well be a process – a series of repeatable actions consistently taken by a company as part of a security and privacy compliance program.

A. Standards under State Laws.

1. Database Breach Notification Laws. In 2002 ,California was the first state to pass a database breach notification law.[27] As of May 26, 2009, forty-four (44) states, the District of Columbia, Puerto Rico and the Virgin Islands had enacted some form of a database breach notification act protecting personal information.[28] Generally these laws do not require specific security measures. However, they require that a company disclose a data breach to those individuals whose data was compromised.[29] The cost of complying with these laws, both from a monetary as well as a publicity perspective, becomes a key factor in creating a security program. Several of these laws promote encryption by not requiring that a company notify customers of a breach if the affected data was encrypted.[30]

2. Nevada Data Encryption Law. In 2006, Nevada enacted a database breach notification law that provided an exemption for encrypted data.[31] More recently, in 2008, Nevada passed a law that requires that personal information transmitted electronically outside of the secure system of a business be encrypted.[32] The Nevada law does not provide any additional guidance as it does not specify any minimum standards for encryption.

3. Massachusetts Data Security Regulation. In 2008, Massachusetts issued comprehensive regulations designed to safeguard residents' personal information.[33] The Massachusetts regulations require that personal information be encrypted during transmission over a public network or wirelessly. The Massachusetts regulations also require that personal information on portable devices (e.g., laptops, flashdrives) be encrypted. In addition to mandating encryption, the Massachusetts regulations go further and require a "written, comprehensive information security program."[34] The security program must be reasonably consistent with industry standards and contain administrative, technical and physical safeguards to ensure the security and confidentiality of records containing personal information. The security program must include the following elements:

(a) designating an individual to maintain the information security program;

(b) identifying and assessing reasonably foreseeable risks;

(c) developing security policies for employees that address how employees can keep, access and transport personal information outside of the business premises;

(d) imposing disciplinary measures to enforce the program rules;

(e) preventing terminated employees from accessing personal information;

(f) protecting personal information provided to third party providers;

(g) limiting the amount of personal information collected, how long it is retained and who can access personal information;

(h) identifying where personal information is located in order to verify that the security program applies to all personal information;

(i) implementing physical access controls;

(j) monitoring the security program;

(k) reviewing the scope of the security measures on at least an annual basis or whenever there is a material change in business practices;

(l) documenting responses to breach incidents; and

(m) implementing a security system that includes:

(i) secure user authentication protocols,

(ii) secure access control measures,

(iii) encryption of personal information transmitted across public networks and all data transmitted wirelessly,

(iv) reasonable monitoring for unauthorized access or access to personal information,

(v) encryption of all personal information stored on portable devices;

(vi) firewalls for Internet-connected devices that contain personal information,

(vii) reasonably up-to-date patches and anti-virus software and

(viii) computer system security training.[35]

The Massachusetts regulations, which include more specifics about the requirements of the required data security plan, are attached as **Appendix A**. These regulations are currently set to become effective as of January, 2010.

4. California Health Care Privacy Laws. In 2009, California enacted two health care privacy laws. The first law requires that healthcare providers establish and implement administrative, technical, and physical safeguards to protect the privacy of patient information and reasonably safeguard confidential medical information from data breaches.[36] The law also establishes the Office of Health Information Integrity within the California Health and Human Services Agency, which has the power to fine violators and also recommend them to other agencies for further review.[37] The second law imposes similar standards on clinics and health facilities. Both bills authorize fines ranging from $25,000 to $250,000.[38]

5. New York Security Breach Law and Business Privacy Guide. In 2007, New York Attorney General Cuomo entered into the state's first settlement under New York's Information Security Breach and Notification Act.[39] Under this law, a business must notify customers of data security breaches immediately following its discovery of the breach.[40] CS STARS, a claims management company, waited for seven weeks before notifying approximately 540,000 New York customers that their electronic personal information had been compromised.[41] Without admitting to a violation of New York's law, CS STARS agreed to pay the Attorney General's office $60,000 for investigation costs and to implement increased privacy and security measures.[42] This landmark settlement may motivate businesses that had previously ignored New York's breach notification requirements to comply with the state's law.

In 2008, New York Governor David Paterson and the state's Consumer Protection Board issued a Business Privacy Guide.[43] The guide recommends that businesses adopt written policies to protect private customer and employee information.[44] Businesses are additionally encouraged to identify data collection and storage practices, plan their responses to data breaches and educate customers, clients, and employees about their privacy policies.[45]

6. New State Privacy Laws Under Consideration in 2009. Many state legislatures are considering enhanced privacy and data security bills in 2009. In New Jersey, a bill under consideration would vastly expand liability under the state's existing data breach notification law. After a breach of customers' credit card data, businesses would be liable to financial institutions for the costs incurred by them in further protecting those customers' personal information.[46] In Missouri, a bill under consideration would require that all businesses that have electronic private customer information notify each customer within thirty days of any data breach.[47] Further, this bill would create criminal penalties for violations of data breach notice laws.[48]

B. Standards under Federal Gramm-Leach-Bliley (GLB). Sections 501 and 505(b) of GLB required the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision (collectively, the "Federal Banking Agencies") to establish appropriate standards for financial institutions with respect to administrative, technical and physical safeguards for customer records and information.[49] The Interagency Guidelines Establishing Information Security Standards (the "Guidelines") establish these standards. [50]

As stated in GLB, and recited in the Guidelines, these safeguards are to: (i) ensure the security and confidentiality of customer records and information, (ii) protect against any anticipated threats or hazards to the security or integrity of such records, (iii) protect against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer, and (iv) ensure the proper disposal of customer information and consumer information.

To meet its stated purpose, the Guidelines provide both substantive and procedural standards for creating, implementing, and maintaining a comprehensive information security program. The substantive objectives of information

security programs are only generally defined by the Guidelines. The steps required for developing and implementing an information security program, however, are set forth with more particularity and most of the Guidelines concern this procedural aspect. The steps, as chronologically arranged within the Guidelines, include the following:

1. Involving the board of directors;

2. Assessing risks;

3. Managing and controlling the risks;

4. Overseeing service provider arrangements;

5. Adjusting the program as circumstances change;

6. Reporting back to the board; and

7. Implementing the standards.

For a more in-depth discussion of the requirements of the information security program, see **Appendix B** to this article.

In order to clarify certain aspects of implementing an information security program that complies with the terms of the Guidelines, the Federal Banking Agencies created two additional publications. First, the "Small-Entity Compliance Guide" summarizes the obligations of financial institutions to protect customer information and illustrates how certain provisions of the Guidelines apply to specific situations.[51] Second, the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" describes appropriate elements of a financial institution's response program designed to address incidents of unauthorized access to sensitive customer information.[52]

With respect to service providers, the Guidelines provide three charges for each financial institution. First, the institution must exercise "appropriate" due diligence in

selecting its providers. Due diligence should include a review of the measures taken by a service provider to protect customer information. It should also include a review of the controls the service provider has in place to ensure that any subservicer used by the service provider will be able to meet the objectives.

Second, the institution must require its service providers, by contract, to implement appropriate measures designed to meet the objectives. This provision does not require a service provider to have a security program in place that complies with each paragraph of the Guidelines. Because the focus is on compliance with the objectives, there is some flexibility for a service provider's information security measures to differ from the program that the contracting financial institution implements. The precise terms and language of service contracts are left to the parties involved.

Third, depending on the risk assessment, the institution may need to monitor its service providers to confirm that they have satisfied their contractual obligations to meet the objectives. This monitoring should include reviews of service providers, such as audits or summaries of test results. Monitoring does not necessarily require on-site inspections, but can instead be accomplished, for example, through the periodic review of the service provider's associated audits, summaries of test results, or equivalent measures of the service provider. Institutions should arrange to have these materials for review through contracts or other agreements.

As a caveat, a financial institution need only monitor its outsourcing arrangements if such oversight is indicated by the institution's own risk assessment. For example, where service providers are financial institutions who are already subject to the Guidelines, or are otherwise subject to other legal and professional standards that require them to safeguard the institution's customer and consumer information, then the institution may take these factors into account.

C. Standards under HIPAA. HIPAA governs the use of protected health information ("PHI"), which the act defines as individually identifiable health information.[53] HIPAA is comprised of two rules, the HIPAA "Privacy Rule" and the "Security Rule." The Privacy Rule controls companies' use of PHI in general (regardless of whether it is electronic or not). The Security Rule complements the Privacy Rule by adding additional requirements for the maintenance of electronic health information.[54]

1. Requirements under HIPAA. HIPAA requirements apply to "Covered Entities" and "Business Associates." Covered Entities include generally health plans, health care clearinghouses and certain health care providers.[55] Under HIPAA, Business Associates are businesses that perform certain services for Covered Entities involving the use or disclosure of PHI. A Covered Entity is required to enter into a contract with a Business Associate to obtain assurances regarding the Business Associate's proper use, disclosure and safeguarding of PHI. Business Associates face substantial contractual obligations through this contract, called the "Business Associate Agreement."[56]

The Business Associate Agreement requirements include restricting the use and disclosure of PHI; reporting violations to the Covered Entity; ensuring that agents and contractors of the Business Associate comply with the same restrictions applicable to the Business Associate; providing access rights to the individual in accordance with the Covered Entity's obligations to provide such access; keeping books and records relating to the use and disclosure of protected health information; returning or destroying PHI at the end of the agreement; and using appropriate safeguards to prevent the use or disclosure of PHI.[57]

The Privacy Rule requires Covered Entities to take the following actions:

1. Provide individuals with notice and certain rights regarding their protected health information;

2. Limit the use and disclosure of protected health information;

3. Obtain authorization from an individual to use or disclose protected health information;

4. Contract with service providers to provide assurances regarding proper use, appropriate disclosure and appropriate safeguards; and

5. Implement policies and procedures to protect protected health information including: appointing a privacy officer, training the Business Associate's workforce, implementing safeguards and a complaint process.[58]

The Security Rule requires that Covered Entities implement administrative, physical and technical safeguards to protect the security of electronic protected health information. Some of these safeguards are required and others are recommended. These are listed in Appendix A to the Security Rule and attached here as **Appendix C.**

2. Requirements under the HITECH Act. Title XIII of the American Recovery & Reinvestment Act of 2009 ("ARRA"), known as the Health Information Technology for Economic and Clinical Health ("HITECH") Act, greatly expands the HIPAA obligations of both Covered Entities and Business Associates. The HITECH Act now imposes direct civil and criminal penalties on Business Associates for certain security and privacy violations under HIPAA.[59] Business Associates are now subject to the majority of the Security Rule, and as a result they will be required to implement and maintain certain security policies and procedures, appoint a security officer and provide related training.[60] In addition, the HITECH Act provides that Business Associates may use and disclose PHI *only* to the extent that such use or disclosure complies with certain requirements in Business Associate Agreements.[61] Effectively, by way of this statutory tie to certain contractual provisions, Business Associates must directly comply with aspects of the Privacy Rule. Moreover, the HITECH Act specifically requires that Covered Entities and Business

Associates modify their existing Business Associate Agreements to incorporate the new Security Rule and Privacy Rule requirements of the Act.[62]

Covered Entities and Business Associates will also be subject to new notification requirements.[63] For example, Covered Entities must make certain notifications within 60 calendar days of discovering a breach of "unsecured" PHI.[64] On the other hand, if PHI is "secured" by an approved methodology (e.g., data encryption or data destruction practices), these notification requirements should not apply to Covered Entities and Business Associates.[65]

The HITECH Act also expands enforcement rights so state attorneys general may bring civil actions in federal court if they have "reason to believe" that "one or more of the residents of that State has been or is threatened or adversely affected" by a violator. Such actions may be brought for injunctive relief or statutory damages, as well as attorneys' fees.[66] The new legislation significantly increases the existing civil monetary penalties for each violation. Civil penalties, which are based upon the cause of the violation and the violator's level of knowledge regarding the violation, generally range from $100 to $50,000 per violation, with caps of $25,000 to $1.5 million for all violations of a single requirement in a calendar year.[67] These increased penalty provisions are effective immediately.[68] In contrast, other provisions will become effective within a year of the legislation (i.e., February 2010), two years after the enactment of the legislation, or after related regulations are published.[69]

3. Recent Changes in Enforcement. The U.S. Department of Health and Human Services ("HHS") has begun proactively enforcing healthcare data protection requirements. In 2008, HHS entered into its first Resolution Agreement with a potential violator of HIPAA's Privacy and Security Rules. In 2005 and 2006, Providence Health and Services ("Providence") lost private electronic health information for hundreds of thousands of customers.[70] In conjunction with this breach, on July 15, 2008, Providence

agreed to pay HHS $100,000 and to implement a corrective action plan which includes increased physical and technical safeguards for transporting and storing electronic media containing patient information and additional training for employees.[71] Providence also agreed to conduct audits of its facilities and submit compliance reports to HHS for three years following the agreement.[72] Though this is the first ever financial payment made to HHS for HIPAA violations, it may signal a shift towards more aggressive enforcement by HHS in the future (especially in light of the expanded enforcement rights under the HITECH Act).

D. Standards under Sarbanes-Oxley. The Sarbanes-Oxley Act and implementing regulations ("SOX")[73] have caused many publicly traded companies to more carefully scrutinize their service provider arrangements, particularly as they bear on internal controls and financial statements. Section 404 of SOX requires that entities establish adequate internal controls and auditing procedures that are certified by management regarding the financial statements of an entity. SOX addresses information security in two ways: first through the requirement of establishing information security processes and audit procedures to protect corporate information, and second through the requirement of accurately reflecting the diminished value of intangible assets because of a security failure or breach, which would include breaches involving private information. While the focus of the SOX requirements is on data security as it affects financial statements, it is possible that a security breach involving private information could lead to a conclusion that adequate security and internal controls have not been established.

E. Standards from FTC Enforcement Actions. Over the past several years, the FTC has aggressively enforced actions against corporations suffering security breaches that reveal consumer information.[74] As of June 18, 2009, the FTC has brought twenty-three cases to challenge data security practices by companies handling sensitive consumer information. While the FTC has attempted to be vigilant in ensuring the safety of consumer information, the

FTC has at the same time been reasonable as institutions have sought to implement measures to comply with FTC regulations. For example, in October 2007, the FTC finalized its "Red Flag" regulations, which require that financial institutions and creditors "develop and implement written identity theft prevention programs that identify relevant patterns, practices, and specific activities that are 'red flags' for possible ID theft" by November 1, 2008.[75] However, in October 2008, the FTC announced that it would delay enforcement of the Red Flag regulation because many institutions which would have fallen within the jurisdiction of the regulation were unaware of the expanded jurisdiction of the regulation and thus unaware of their responsibilities under it.[76]

Under the authority of Section 5(a) of the FTC Act,[77] the FTC has stated that a "fail[ure] to employ reasonable and appropriate security measures to protect [consumer] information" is an unfair practice.[78] The FTC has repeatedly cited four to six specific types of lax information security in their filed complaints, and the resulting consent orders demand virtually identical corrective actions by each company. Several of the most recent cases are discussed in **Appendix D** to this article: CVS Caremark, Genica Corporation, Premier Capital Lending, Reed Elsevier, TJX, ValueClick, Goal Financial, Life is Good Retailer, American United Mortgage Company, Guidance Software, CardSystems Solutions, DSW and BJ's Wholesale Club.

Nearly all of the FTC's Section 5(a) complaints against companies include at least one of the following six practices. The fifth and sixth practices are alleged against companies in the most recent complaints. "[T]aken together, [these practices] did not provide reasonable security for sensitive customer information," although the FTC has not designated any one practice as dispositive in assessing a Section 5(a) violation.[79]

1. Easy Network Access – Failing to limit wireless access to their networks, and/or failing to limit their networked computers' access to each other and the Internet.[80]

2. No Breach Detection – Failing to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.[81]

3. Unnecessary Storage – Creating unnecessary risks to the information by storing it, often when they no longer had a business need to keep the information.[82]

4. Weak Encryption/Passwords – Storing and/or transmitting information in an unencrypted format, or using weak/commonly known user IDs and passwords, to protect information stored on their networks.[83]

5. Inadequate Defense to Known Attacks – Failing to adequately assess the vulnerability of [their] computer network to commonly known or reasonably foreseeable attacks, including 'Structured Query Language' injection attacks, and not implement[ing] low-cost, and readily available defenses to such attacks.[84]

6. Unsafe Information Disposal – Failing to dispose safely of customer and employee information.[85]

In nearly all security breach cases since 2005, the FTC's consent agreements have required alleged violators to take three types of corrective actions, which have been standardized in enforcement settlement agreements with nearly identical language. These three standard corrective actions are:

1. Security Program – Establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.[86]

2. Auditing and Assessment – Obtain an independent third-party audit of its security program, every other year for a ten or twenty–year period, to certify that the program is sufficient to protect its consumers' confidential information.[87]

3. Compliance and Reporting – Maintain, and upon request make available to the FTC, records relating to compliance, including documents prepared internally or externally that may call into question compliance with the consent order and documents relied upon to prepare the required third-party audit; notify the FTC of any changes in corporate structure; and provide all new directors, officers, and executives of the corporation a copy of the consent order.[88]

The Security Program provisions are worth additional examination. These programs must "contain administrative, technical, and physical safeguards appropriate to [the company's] size and complexity, the nature and scope of [the company's] activities, and the sensitivity of the personal information collected . . . ."[89] Specifically, companies creating these security programs must implement four safeguards:

1. Designated Security Coordinator – "[T]he designation of an employee or employees to coordinate and be accountable for the information security program."[90]

2. Risk Assessment – The development of a comprehensive risk assessment of major areas of operation, "including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failure[s]."[91]

3. Safeguard Implementation – "[T]he design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures."[92]

4. Ongoing Evaluation and Adjustment – Evaluation and adjustment of this security program in light of test results, changes in the company's business, "or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its

information security program."[93]

Fortunately for companies deciding how to upgrade their information security, the FTC has entered into nearly uniform consent agreements with companies engaged in a nearly uniform pattern of unsecure practices. Although the FTC has not stated that a single precaution will avoid Section 5(a) "unfair practice" liability, it seems to have established guidelines that should help avoid liability in the unfortunate event of a security breach.

1. Limit Network Access – Companies should set up strong encryption for their wireless networks, and computers' access to (1) internal and external networks, (2) the Internet, and (3) other networked computers should be kept to the absolute minimum necessary for essential tasks and functions. For example, a computer used only for performing a single task at an individual retail store should not have full Internet access, or full access to a broader multi-store network.

2. Install Robust Security Software – Companies should invest in software systems capable of detecting security breaches, and they should periodically review these systems to ensure the ongoing protection of customer information.

3. Limit Unnecessary Storage – Customer information should be erased as soon as it is no longer needed.

4. Create Strong Passwords and Use Tough Encryption – Companies should make sure that any transmission or storage of customer data is protected by difficult passwords and encryption.

5. Stay Informed About Well-Publicized Hacking Techniques – IT security personnel should stay informed about the latest techniques and tactics used by hackers. The FTC does not require companies to protect against novel attacks that are difficult to predict or anticipate. Companies will be held liable, however, if they do not use

cost-efficient, well-known defenses against well-publicized hacking techniques.

The FTC has made no secret of its desire to protect consumers from identity theft. Over the past four years, the FTC has laid down relatively clear guidelines as to which practices are punishable as violations of Section 5(a) of the FTC Act, and companies wishing to limit their liability would be wise to avoid the costly mistakes already made by other corporations. Although protections against hackers and identity thieves can never be perfect, implementing procedures stipulated in recent FTC consent orders may prevent unnecessary liability should an attack occur.

F. Standards from Cases. There are several recent cases that address standards of conduct and potential liability in the security and privacy areas. In *Caremark International*, a Delaware court stated that "it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility."[94] This case acknowledges a duty of the board of a corporation to see that the corporation has an adequate information system. In another recent case, a Michigan appeals court found that a union had a duty to protect an information system from reasonably foreseeable breaches, and the union was negligent in not doing so.[95]

In *Guin v. Brazos Higher Education Service*, a federal court held that the duty to provide reasonable security had been satisfied where the defendant had implemented the proper safeguards as required by GLB, including a risk assessment, security program and security measures, even though there had been a security breach.[96] The court also rejected the plaintiff's argument that encryption of data was legally mandated. This finding is an interesting contrast to the FTC consent decrees and actions discussed above which found a lack of encryption of data to be actionable.

In *Kahle v. Litton Loan Servicing L.P.*, the U.S.

District Court for the Southern District of Ohio held that the cost of enrolling in a credit protection program due to a fear of identity theft did not constitute a sufficient damage to support a negligence claim arising from a data breach incident.[97] The decision follows the general rule that the risk of future injury is not a sufficient harm to support a negligence claim against a financial institution.

Most recently in *Pisciotta v. Old Nat'l Bancorp*, the U.S. Court of Appeals for the Seventh Circuit affirmed the decision for the defendant issued by the lower court.[98] The court held that costs for credit monitoring, to guard against some future, anticipated harm, are not compensable injuries under Indiana law.

G. Standards from Agencies and Non-Governmental Organizations.

1. General Standards.

Federal agencies and non-governmental organizations have also issued voluntary privacy and data security standards. These standards are useful for companies trying to craft "reasonable and appropriate security measures," and thus reduce the probability of security incidents (and any associated liability under state or federal law).

In 2008, the National Institute of Standards and Technology ("NIST"), a non-regulatory federal agency within the U.S. Department of Commerce, issued a Performance Measurement Guide for Information Security.[99] The guide recommends that organizations implement security controls that include management, operational and technical safeguards to protect confidential information.[100] In 2006, a similar NIST guide provided minimum security requirements for federal agencies.[101]

Likewise, two non-governmental organizations, the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC") have jointly issued standards recommending information security management controls for all organizations. Their 2009

ISO/IEC 27000-series of standards advises organizations on creating and implementing information security systems and evaluating the success of these systems.[102]

2. Industry Specific Standards.

Another non-governmental organization, the Payment Card Industry Security Standards Council ("PCI SSC"), has developed a mandatory, industry specific standard to protect confidential consumer information. Payment Card Industry ("PCI") Data Security Standards ("DSS") is an industry standard created by the PCI SSC to "encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally."[103] PCI requires that all companies that process, store or transmit credit cardholder data be PCI DSS compliant. PCI DSS is divided into six control objectives that combined contain twelve high level requirements:

(a) Build and Maintain a Secure Network

(i) Install and maintain a firewall configuration to protect cardholder data

(ii) Do not use vendor-supplied defaults for system passwords and other security parameters

(b) Protect Cardholder Data

(i) Protect stored cardholder data

(ii) Encrypt transmission of cardholder data across open, public networks

(c) Maintain a Vulnerability Management Program

(i) Use and regularly update anti-virus software

(ii) Develop and maintain secure systems and applications

(d) Implement Strong Access Control Measures

(i) Restrict access to cardholder data by business need-to-know

(ii) Assign a unique ID to each person with computer access

(iii) Restrict physical access to cardholder data

(e) Regularly Monitor and Test Networks

(i) Track and monitor all access to network resources and cardholder data

(ii) Regularly test security systems and processes

(f) Maintain an Information Security Policy

(i) Maintain a policy that addresses information security

PCI DSS sets forth testing procedures and, unlike the standards from most laws and regulations, provides very specific minimum requirements. For example, to provide for accountability, all users must be assigned a unique ID. Additionally, local users must have at a minimum a password, remote users must use two-factor authentication and all passwords must be encrypted using strong encryption during transmission and storage.[104]

H. Common Elements of the Various Standards. Developments in this area point to a simple emerging principle: that reasonable security measures are about good and reasonable processes, not a particular security solution. And as with manufacturing processes,

where one element breaks down and production comes to a halt, security processes will not be perfect, and will not always be uninterrupted. But if perfection is not the standard, what activities demonstrate a good and reasonable security process that enables privacy compliance? The following steps outline a suggested process for implementing a security program that minimizes the risk of privacy violations.

1. **Security and Privacy Officers.** Assign a Security and/or Privacy Manager to coordinate the process.

2. **Internal Assessment.** Assess the assets and risks to personal information in each area of the company's operations. Identify current protections and controls in use. It may be helpful to have legal counsel coordinate and oversee this type of internal assessment, including, if appropriate, contracting with appropriate external consultants and resources who specialize in these types of assessments. In this way, the results of the assessment can possibly receive attorney-client privilege. Since it will be impossible to completely mitigate each risk, it will be necessary to identify the likelihood of a risk, the potential damage that an incident of that nature could cause, and the sufficiency of existing or future processes and safeguards to mitigate or attempt to prevent the risk. Some levels of risk may be acceptable, especially given the reality that no company has unlimited resources to put toward perfect security. In addition to gathering the facts regarding the company's current assets and risks, the other important outcome of the assessment will be to prioritize risks and mitigation efforts to address those identified risks which are unacceptable.

3. **Process Design.** Design a security and privacy protection program that takes into account the following areas of required action:

(a) Adopting system access and change controls;

(b) Adopting physical access controls over facilities and physical access to systems and records;

(c) Encrypting data when in transit or when on systems or networks where unauthorized individuals may gain access;

(d) Using technology solutions like firewalls, monitoring software and intrusion detection products;

(e) Implementing incident response plans to maintain business continuity, to remedy security breaches involving unauthorized access or use of information and to minimize the impact of disasters;

(f) Employee screening for jobs involving access to sensitive information and appropriate employee training and education emphasizing security program elements that employees are responsible for implementing (such as keeping passwords secret, locking files and laptops, not downloading unauthorized software, etc.);

(g) Developing a Service Provider Diligence, Contracting, Monitoring and Reviewing program as a sub-component of your security program; and

(h) Developing appropriate records and data retention and disposal measures, and ensuring that they are followed.

4. **Testing and Monitoring.** Test and Monitor all areas of the program, especially key controls. Consider whether to hire a third–party security auditor to help in testing and refining the program. The legal department should oversee all audits and testing results so that those materials receive attorney-client privilege.

5. **Evaluate and Evolve.** Evaluate and adjust the program on an ongoing basis. This entails keeping up with both internal incidents and risks (acquisitions, new product lines, changing workforce patterns (e.g., work from home models), as well as external developments by way of new threats, other security incidents and new technologies and practices adopted in the company's industry.

IV. OUTSOURCING (ONSHORE AND OFFSHORE)

If you are in a regulated industry such as healthcare or financial institutions, then you already know that you cannot "outsource" responsibility for legal and regulatory compliance. The ultimate responsibility and liability for such compliance rests with the regulated entity. This is as true for privacy compliance as it is for SOX compliance. Some companies tend to throw privacy compliance "over the wall" to the service provider, and hope that they do not have to address it again. This is a mistake that can lead to privacy violations, regulatory enforcement and embarrassment for the neglectful company.

One might expect that outsourcing to an offshore service provider presents additional legal and regulatory compliance issues regarding privacy and security. That is not the case, however, except in three potential sets of circumstances: (1) where a government entity is the customer,[105] (2) where your company has government contracts, in which case you will need to review those contracts for any applicable restrictions, or (3) in certain cases involving taxpayer data regulated by the IRS. As of January 1, 2009, U.S. tax return preparers have been required to obtain taxpayers' consent for any disclosure of tax return information to offshore preparers, even if the taxpayers' Social Security numbers are "fully masked or otherwise redacted."[106] Other than in those limited circumstances, there are no significant differences in privacy compliance requirements under U.S. laws for businesses who outsource to an offshore provider versus an onshore one.[107] The laws that apply to a business using an outsourcing service provider in the U.S. apply equally to use of an outsourcing service provider outside of the U.S.

There are, however, a few important considerations when outsourcing to an offshore service provider who will handle personal information. First, the business must consider whether the laws of the country or countries from which the service provider will provide services will apply to or otherwise affect privacy compliance. For example, data that is transferred to, or accessed from, an EU member state

may become subject to the EU data protection laws, even though the data originates outside of the EU. Second, a business needs to evaluate and consider whether the laws of the offshore service provider's country (or lack of protective laws) increase the risk to the business in the event of a privacy or security breach, and whether those laws will negatively affect enforcement of rights. Third, a business must consider the extent to which an offshore service provider makes oversight and management more challenging, and must devise ways in which to address this practical difficulty. Finally, a business must consider the political and public relations risks that it may incur as a result of a privacy or security breach regarding an offshore service provider.[108]

V. COMPLIANCE THROUGH SERVICE PROVIDER CONTRACTING

As discussed above, managing privacy risks with service providers requires that a company have a security and privacy process generally, with specific steps that pertain to service providers. At a high level, these steps include:

1. Appropriate service provider diligence and selection;

2. Implementing security standards and privacy requirements through appropriate contractual clauses; and

3. Monitoring performance and adherence to the standards and process.

Whether onshore or offshore, businesses who use outsourcing service providers where personal information will be collected, processed, accessed, stored or transferred must perform due diligence on the service provider at the contracting stage, as well as continue meaningful oversight during the term of the contract. It is also not enough to rely on a few high level sentences in a service provider contract to establish the sufficiency of privacy and security. An outsourcing customer needs a standard set of terms and conditions regarding personal information that are tailored for use with a service provider. Not all of the terms will be

required in all situations, but any service provider who handles personal information for you has the potential to cause you problems if the personal information is not properly handled and protected.

And, while you cannot outsource responsibility for your compliance obligations, you can and should ensure that you and your provider understand the following topics (and have documented such understanding in the contract):

Specific Privacy Requirements for Personal Information – the specific privacy requirements to be performed by your service provider (including how the service provider may and may not use personal information);

Security Requirements – your security requirements and the service provider's security practices to monitor and prevent security breaches and to protect your business;

Change Control – a process for reviewing any process or system changes that may impact security or privacy issues;

Reporting Requirements – your reporting requirements for privacy compliance;

Audit Requirements – your audit requirements;

Subcontracting Approval Rights and Flow Down of Provisions – your rights to approve any subcontracting and requirements that all subcontractors agree to the same security and privacy terms as your primary service provider;

Incident Plans – what you will do if your service provider suffers a security/privacy breach, including business continuity and disaster recovery plans;

Changes in Requirements – responsibilities for monitoring changes in privacy laws and regulations,

and adjusting service requirements to meet such changes;

Liability – liability for breaches of privacy and/or security; and

Costs – what will be done as part of the services, and which requirements may result in extra charges by the service provider.

A. <u>Specific Privacy Requirements For Personal Information</u>. The starting point for defining service provider privacy requirements is to understand your own privacy requirements. This requires that you know what privacy laws and regulations apply to you, and that you understand and document the requirements. From that point, you need to determine based on the services your service provider will provide which of your requirements apply to your service provider. For example, if your service provider will perform human resources services, your service provider will have access to huge amounts of sensitive personal information. If your service provider is performing procurement services, your service provider may have some personal information (individual names at the businesses from which you procure things), but the nature of this information and the risks it presents are far less sensitive from a privacy perspective.

Unless you have well-defined service provider requirements in your privacy and security policies, it is usually not enough to say "service provider must comply with company's privacy and security policies." Similarly, requiring your service provider to use "reasonable and appropriate technical and security measures" as a means to prove compliance with privacy laws may not be enough. You should be specific about the obligations your service provider will have regarding personal information. These specifics should answer the following questions:

- How may the service provider use personal information? (normally solely for the purpose of providing the services for the benefit of

customer, and for no other purposes)

- Where will the personal information be stored and processed?

- How long will personal information be retained? (usually, per customer defined requirements)

- Is the service provider permitted to transfer the personal information to other locations? Other countries? Or only on instruction from the customer?

- As between the customer and service provider, who owns the personal information?

- How is customer permitted to access its personal information, when and on what conditions, if any?

- Will service provider agree that it will not hold personal information or otherwise prohibit access to it for any reason whatsoever, including during the pendancy of any disputes?

- Is service provider obligated to assist customer in customer's compliance with all privacy and related security laws and regulations applicable to customer? Will service provider commit to take all necessary steps and measures and to provide cooperation with customer so that customer may ensure compliance? Who will pay for modifications to the services to comply with changes in requirements?

- Is service provider required to immediately notify customer in the case of any personal information loss or unauthorized access (attempted or actual)?

- How will customer receive its personal information upon expiration or termination of the agreement, including form and format of the data, and/or destruction and certification requirements?

- What procedures will the service provider follow for any personal information reconstruction after loss or error correction?

- What process will customer and service provider follow for access to personal information by data subjects, if such access is required by law or by the customer?

- What are the permitted reasons for disclosure of the personal information to any party other than customer? What is the process if service provider receives a subpoena or other request for disclosure?

- What obligation does service provider have to inform employees and contractors of customer's privacy requirements?

- What other specific requirements will exist due to legal or regulatory requirements of the customer? (e.g., compliance with GLB and related regulatory requirements)

- Will service provider have to sign a Business Associate Agreement with customer for HIPAA compliance?

- Will service provider have to sign EU approved data protection clauses or use some other approved means of processing and transferring data under the EU regime?

B. **Security Requirements.** Your own security requirements and practices are often the right starting point for defining service provider security requirements.

However, you need to determine whether your requirements fit the particular service provider situation. The service provider may offer a standard package of services that may not easily be modified to fit your particular security requirements, at least not without incurring significant cost. For example, you may desire that service provider dedicate a portion of its shared services facility solely for your work, that it house your computer servers there, and that only approved service provider personnel may have access to this area. These requirements may be great for security, but may break the outsourcing budget.

While it is good to define specific security requirements, such as use of passwords, proper network administration, firewalls, encryption, etc., it is also helpful to refer to applicable industry standards to fill in the gaps for requirements. Subject matter experts and/or security professionals can assist you in referencing appropriate industry standards that you may require your service provider to be certified in or to follow. For example, some of the following standards are appropriate to reference in certain outsourcings involving data center operations: ISO/IEC 27002, ISO/IEC 27001, ITIL and CMM standards. Generally, the existing privacy laws and regulations do not require perfection or complete fail-safe security. Rather, they tend to require processes that are reasonable and appropriate given the nature of the personal information and the circumstances.

Depending upon the nature of the services and the amount of personal information the service provider will handle, you should also consider the following:

- Will the service provider use a shared services facility where your personal information will be mixed with that of other customers? If so, what additional security precautions should you require?

- Will your personal information be stored on servers that can be accessed by anyone other than authorized service provider personnel

and your own authorized personnel? If so, who can access it, and what security precautions are taken to partition server and data access?

- Does your service provider re-purpose computer servers and storage data? If so, how does the service provider ensure that personal information is completely erased before re-use?

- What physical security procedures does service provider follow at its facilities to prevent unauthorized access?

- What network security does service provider use to prevent unauthorized access to computer infrastructure and databases?

- Does service provider do penetration testing in its data centers that will contain your personal information? Will it share the results of such tests with you?

- Will service provider need to access any of customer's systems? If so, what are the security requirements for such access?

- Will service provider keep personal information encrypted?

- How will service provider protect against data loss, misuse, alteration, destruction and unauthorized access?

- If personal information is kept in hard copy or tangible (non-electronic) form such as disks or tapes, how are these physical embodiments secured?

- If physical embodiments (e.g., tapes) containing personal information are

transferred from one location to another, how is the transfer accomplished?

C. Reporting Requirements. Reporting is essential to monitoring any outsourcing service provider. It is also important to a business for use in demonstrating its own privacy compliance.

- As the customer, what reports relating to privacy compliance do you have to provide on a regular basis or from time to time?
- What reports will various parts of your business require? (e.g., SOX compliance, auditors, marketing, etc.)
- What obligations will service provider have to create other or ad hoc reports? At what additional cost, if any?
- Will the service provider provide reports on routine monitoring of systems and security?
- Will service provider provide reports on security incidents?
- Will service provider correct erroneous reports at no charge?
- What is the format and means of making the report? (e.g., electronic file, FTP, intranet access, hard copy, etc.)

D. Audit Requirements. Specifying audit requirements is important for any number of compliance programs (e.g., SOX) and is equally important to demonstrate that management is executing oversight of an outsourcing service provider to assure privacy compliance.

- What written procedures and descriptions of controls does service provider have (both for physical facilities access and protection and

for network and infrastructure)?

- Do service provider's procedures and controls satisfy your own control requirements?

- What types of records will customer require access to for audit purposes?

- May customer conduct operational and facility audits to confirm compliance, examine controls and security, and enable customer to comply with applicable privacy laws and regulation?

- Will service provider cooperate with such audits, including providing facility and system access, access to key personnel, etc.?

- Will service provider provide SAS 70 audit reports? What type and to what level? How often? Will the timing match with customer's required time frames for management certification? Will customer have to perform its own SAS 70 audit of service provider facilities to comply with customer requirements?

- Will service provider provide full cooperation for any government or regulatory audits required of customer?

- How will service provider respond to audit issues identified by customer audits? Governmental or regulatory audits? Will service provider correct such audit items at no charge? Will service provider report on such corrections to customer?

- Does service provider conduct its own internal quality assurance and/or security audits?

- Will service provider provide those audit

results, or summary thereof, to customer?

E. <u>Breach Action Plan Requirements</u>. Security breach action plans are necessary due to the proliferation of state database breach laws. Many businesses have not yet developed such a plan, but it is better to do so before the chaos of a security breach occurs. The internal business plan will cover multi-step responses with the objective to identify and stop the cause of the breach, comply with legal requirements, minimize damages to the affected individuals, provide notice to affected individuals, notify regulators (where required), minimize damages to the business, notify and engage appropriate business officers and departments, engage external consultants and PR professionals, and other similar crisis management steps. A business should assess which parts of the internal plan require involvement of the service provider, and the contract should provide for such involvement. The contract should also answer the following questions:

- Does service provider have an internal response plan for security breaches?
- Has service provider implemented this plan before?
- Does customer have a response plan? If so, which parts require service provider cooperation?
- Does service provider need to participate in or follow any portions of customer's response plan?
- What is the process for notifying customer of an actual or attempted security breach?
- Which party will notify any regulatory authorities of a breach?
- Which party will notify affected individuals of a breach?

- Which party may approve of the notices to individuals?

- Which party may speak to the media about or comment on the breach? May a party do so without the approval of the other party? May it name the other party?

F. <u>Changes in Privacy Law and Regulation</u>. All successful outsourcing relationships require flexibility to accommodate change. In the area of privacy compliance, change is inevitable, both in terms of laws and industry standards. The contract should provide for the following areas:

- Which party is responsible for monitoring privacy law and regulatory changes?

- Which party is responsible for re-defining requirements relating to such changes?

- What is the contractual process for implementing such changes?

- What if the parties differ on interpretation of legal requirements? Which party wins?

- What obligation does service provider have to keep its security measures up to date with industry standards?

- Will service provider review changes in industry standards with customer? Will service provider implement such changes in industry standards at no charge to customer?

- Do customer's legal requirements require any special training for service provider employees?

G. <u>Liability</u>. This is perhaps the most difficult of all of the topics addressed in this article. Positions of

customers and of service providers vary widely on allocation of liability and responsibility for security breaches. The customer will desire complete unlimited liability (including consequential damages) and corresponding indemnities for security and privacy breaches, much the same way that confidentiality breaches have traditionally been handled in outsourcings. The service provider may seek to limit its liability for privacy and security breaches, at least to the extent that service provider can demonstrate that the breach occurred <u>despite</u> the service provider's compliance with contract obligations. This is a rapidly developing area that will continue to be influenced by developing law, and customer and service provider experiences. Among the more important questions regarding liability for privacy and security breaches are:

- Is a breach of confidentiality the same as a breach of privacy and/or security?

- Are consequential damages excluded? If so, are damages for breaches of confidentiality and privacy carved out from the consequential damage exclusion?

- What is the appropriate level of service provider liability for a privacy/security breach? Unlimited? Only liable if it did not follow requirements for privacy and security? What if service provider did follow the requirements, but a breach occurs anyway? Should service provider be liable then?

- What damages should be included for a privacy or security breach?

- Customer's own damages?

- Damages for costs of defending and/or settling third-party suits, claims, and investigations?

- Damages for costs of notifying third parties of

breach?

- Damages for costs of cover to remediate breaches and fix problems?

- Damages for governmental fines and penalties?

- Damages for loss of profits, goodwill and loss of reputation?

- Beyond specific requirements in the contract, what will be the effect of references to "gap filler" standards in determining service provider liability?

- What liability of the service provider should apply to criminal or willful misconduct of employees? Contractors and agents? Unrelated third parties?

- What liability should apply to gross negligence of service provider and its personnel?

H. **Costs.** While it is important to answer the questions above correctly for the business, an outsourcing customer cannot forget that everything has a price. Vendor services are not free. Vendors cannot agree to contract clauses that require material additional work with no means of recouping or at least discussing material additional costs. Businesses will want to be careful to not force additional and unnecessary cost into a service provider's pricing for privacy and security compliance that exceeds business needs. Determining who bears the cost for all of these compliance terms requires much discussion and negotiation between the parties.

- What parts of privacy processes, procedures, security requirements, audits, reports, changes and contingency plans are included in service provider's base price?

- What activities will lead to additional charges, and what is the threshold for such charges? What will the rates be for performing the additional services?

- As between customer and service provider, who is in the best position to bear a cost or a risk and the related costs?

VI. CONCLUSION

It is obvious from the recent developments that security and privacy compliance are significant matters for companies, and need to be taken seriously – at all levels of the organization. Companies facing security breaches or regulatory reviews and actions will be required to demonstrate that they are implementing sound processes aimed at security and privacy compliance. These processes are not about a single solution or particular technology. Instead, they are about demonstrating that a company has assessed its risks, devised processes and approaches to mitigate the most likely and serious of those risks, and implemented those processes and approaches consistently. Ongoing monitoring and adjustments to the processes are equally important. No program will be perfect, but the use of well-designed and consistently applied processes can go a long way toward demonstrating that a company has taken reasonable measures to ensure security and privacy compliance.

APPENDIX A - MASSACHUSETTS DATA SECURITY REGULATIONS

201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

17.01 **Purpose and Scope**

(a) Purpose

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. Further purposes are to (i) ensure the security and confidentiality of such information in a manner consistent with industry standards, (ii) protect against anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud against such residents.

(b) Scope

The provisions of this regulation apply to all persons that own, license, store or maintain personal information about a resident of the Commonwealth.

17.02: **Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

“Breach of security”, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of

personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

“Electronic,” relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

“Encrypted,” the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the office of consumer affairs and business regulation.

“Person,” a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

“Personal information,” a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account; provided, however, that “Personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Record" or "Records," any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

17.03: **Duty to Protect and Standards for Protecting Personal Information**

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. Such comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records. Moreover, the safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns, licenses, stores or maintains such information may be regulated.

Whether the comprehensive information security program is in compliance with these regulations for the protection of personal information, whether pursuant to section 17.03 or 17.04 hereof, shall be evaluated taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information. Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more employees to maintain the comprehensive information security program;

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.

(c) Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.

(f) Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain

such safeguards. After January 1, 2010, prior to permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations.

(g) Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.

(h) Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.

(i) Reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers.

(j) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of

personal information; and upgrading information safeguards as necessary to limit risks.

(k) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(l) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, shall have the following elements:

(1) Secure user authentication protocols including:

(i) control of user IDs and other identifiers;

(ii) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

(iv) restricting access to active users and active user accounts only; and

(v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) Secure access control measures that:

(i) restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(ii) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(3) To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly.

(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices, provided that such person shall have until January 1, 2010 to encrypt personal information on such other portal devices;

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: **Effective Date**

Every person owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall, unless otherwise expressly provided herein, by in full compliance with 201 CMR 17.00 on or before May 1, 2009.

REGULATORY AUTHORITY:

201 CMR 17.00: M.G.L. c. 93H

APPENDIX B – OVERVIEW OF INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

1. IMPORTANT TERMS USED IN THE GUIDELINES

Customer Information – "Customer information" means any record containing nonpublic personal information about an individual who has obtained a financial product or service from the institution that is to be used primarily for personal, family, or household purposes and who has an ongoing relationship with the institution.

Consumer Information – "Consumer information" means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the financial institution for a business purpose. The term also means a compilation of such records. The term does not, however, include any record that does not identify an individual.

Customer Information System – "Customer information system" means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

Service Provider – "Service provider" is defined as any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services *directly to the institution*. This includes a processor that directly obtains, processes, stores or transmits customer information on an institution's behalf. Similarly, an attorney, accountant, or consultant who performs services for a financial institution and has access to customer information is a service provider for the institution.

2. DEVELOPING AND IMPLEMENTING AN INFORMATION SECURITY PROGRAM

Under the Guidelines, financial institutions are expected to create, implement and maintain a comprehensive written information security program. This program is to include administrative, technical and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities.

The objectives of the information security program are nearly identical to the objectives identified in GLB, altered only for the inclusion of the disposal requirement for customer information and consumer information, as required by the FACT Act. The four objectives (the "Objectives") of an information security program under the Guidelines are to:

1. Ensure the security and confidentiality of customer records and information;

2. Protect against any anticipated threats or hazards to the security or integrity of such records;

3. Protect against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer; and

4. Ensure the proper disposal of customer information and consumer information. According to the Guidelines, access to or use of customer information is not "unauthorized" access if it is done with the customer's consent.

In developing and implementing an information security program, an institution must follow a discrete set of steps set forth in the Guidelines: involving the board of directors, assessing risks, managing and controlling the risks (including designing the information security program,

training staff, testing key controls, and implementing a disposal program), overseeing service provider arrangements, adjusting the program as circumstances change, reporting back to the board, and implementing the standards. Each of these steps is discussed in detail below.

2.1 Involving the Board of Directors

According to the Guidelines, the board of directors of a financial institution is required to be involved in information security in that it must: (1) approve the institution's written information security program; and (2) oversee the development, implementation and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management. An institution is not permitted to decide for itself whether to obtain board approval of its program, and the responsibilities of approval and general oversight remain on the board. However, the board may assign specific implementation and management responsibilities to a committee or an individual. Accordingly, the term "oversee" is meant to convey a board's conventional supervisory responsibilities, and not day-to-day monitoring. Day-to-day monitoring of any aspect of an information security program is considered a management responsibility that can be delegated to a committee or individual.

2.2 Assessing Risks

In assessing risks to customer and consumer information, an institution must perform three steps. The institution must: (1) identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and (3)

assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks. Each of these steps must also be applied in connection with the disposal of customer information, as further discussed below.

Once an institution has assessed the risks to customer and consumer information, it must take steps to manage and control risks. Under the guidelines, each financial institution must take the following three general actions to manage and control assessed risks: (1) design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities; (2) train staff to implement the institution's information security program; (3) regularly test the key controls, systems and procedures of the information security program; and (4) develop, implement, and maintain as part of its program appropriate measures to properly dispose of customer information and consumer information. Each of these actions is discussed in greater detail below.

2.3 Designing the Information Security Program to Control the Identified Risks

An institution's information security program must be commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities. The Guidelines identify eleven security measures an institution *must* consider in evaluating the adequacy of its policies and procedures to effectively manage risks. Although not every security measure listed needs to be implemented as part of a security program, an institution must review each security measure and consider whether it is appropriate given the institution's circumstances. If determined that a security measure is to be adopted, the manner in which the security measure is adopted is up to the institution.

The security measures identified in the Guidelines include: access controls, physical access restrictions, encryption, system modification checks, dual control procedures and segregation of duties, attack monitoring, response procedures, and environmental hazard protection. Each of these types of security measures is discussed in greater detail below.

Access controls – Access controls on customer information systems: controls to authenticate and permit access only to authorized individuals, and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means. These access controls should prevent unauthorized access to customer financial information by anyone, whether or not employed by the institution.

Physical access restrictions – This measure involves access restrictions at physical locations containing customer information to permit access only to authorized individuals. Such physical locations include buildings, computer facilities, and records storage facilities.

Encryption – Encryption of electronic customer information that is in transit, or when in storage on networks or systems to which unauthorized individuals may have access.

System modification checks – Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program.

Dual control procedures – This security measure encompasses dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information. Dual

control procedures refer to a security technique that uses two or more separate persons who operate together to protect sensitive information. Under such a technique, both persons are equally responsible for protecting the information and neither can access the information alone. As noted by the Guidelines, dual control procedures are not necessary for all activities, but may be appropriate for higher-risk activities.

Attack monitoring – Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.

Response procedures – Response programs that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies. The Federal Banking Agencies' "Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice"[109] states that, at a minimum, a response procedure should contain procedures for:

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused;

- Notifying the institution's primary federal regulator as soon as possible when it becomes aware of an incident involving unauthorized access to or use of sensitive customer information;

- Filing a timely Suspicious Activity Report (SAR), and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notifying appropriate

law enforcement authorities;

- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and

- Notifying a customer when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it.

The threshold for "sensitive customer information" is extremely low, and is not limited to nonpublic information. Sensitive customer information means a customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, credit card or debit card number, or a personal identification number or password that would permit access to the customer's account. It also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as a username or password, or password and account number.

- Notice to the customer should include the following terms:

- A description of the incident;

- The type of information subject to unauthorized access;

- The measures taken by the institution to protect customers from further unauthorized access;

- A telephone number customers can call for information and assistance; and

- A reminder to customers to remain vigilant over the following twelve to twenty-four months, and to report suspected identity theft incidents to the institution.

Environmental hazard protection – Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage. These measures also include disaster recovery due to technological failures.

2.4 Training Staff

Each information security program should include a training component designed to train employees to recognize, respond to and report unauthorized attempts to obtain customer information. As part of a training program, employees and staff should be made aware both of federal reporting requirements and the institution's procedures for reporting suspicious activities, including attempts to obtain access to customer information without proper authority.

2.5 Testing Key Controls

As part of its information security program the institution should regularly test the key controls, systems and procedures of the program. The type of testing that is performed is left to the discretion of the management, and is not specified in advance by the Guidelines. However, any tests performed by an institution should be either conducted or reviewed by persons who are independent of those who operate the systems (including the management of the systems).

Whether a financial institution should use third parties to either conduct tests or review their results depends upon a number of factors. As noted by the Guidelines, some financial institutions may have the capability to thoroughly

test certain systems in-house and review the test results but will need the assistance of third-party testers to assess other systems. For example, an institution's internal audit department may be sufficiently trained and independent for the purposes of testing certain key controls and providing test results to decision makers independent of system managers. Some testing may be conducted by third parties in connection with the actual installation or modification of a particular program. In each instance, management needs to weigh the benefits of testing and test review by third parties against its own resources in the area, both in terms of expense and reliability.

2.6 Creating an Information Disposal Program

As part of its information security program, a financial institution must develop, implement and maintain appropriate measures to properly dispose of customer information and consumer information. The financial institution must use risk-based measures to protect customer information and consumer information in the course of disposing of it. Accordingly, a financial institution must broaden the scope of its risk assessment to include an assessment of the reasonably foreseeable internal and external threats associated with the methods it uses to dispose of "consumer information," and adjust its risk assessment in light of the relevant changes relating to such threats. In other words, each of the risk-based measures a financial institution undertakes with respect to designing, implementing and maintaining its program to protect its customer information and customer information systems also extends to the *disposal* of customer information and consumer information.

As with aspects of the information security program relating to the protection of customer information and customer information systems, the Guidelines do not provide a prescriptive rule describing proper methods of disposal. The institution is to develop its own method for disposal that

is based on its risk assessment, and which is appropriately suited to the varying circumstances that the institution may confront. It is expected, however, that an institution's information security program ensure that paper records containing either customer or consumer information be rendered unreadable as indicated by the institution's risk assessment, such as by shredding. Further, institutions should recognize that computer-based records present unique disposal problems, namely, that residual data frequently remains on media after erasure. Since that data can be recovered, additional disposal techniques should be applied to sensitive electronic data.

2.7 Overseeing Service Provider Arrangements

With respect to service providers, the Guidelines provide three charges for each financial institution. First, the institution must exercise "appropriate" due diligence in selecting its providers. Due diligence should include a review of the measures taken by a service provider to protect customer information. It should also include a review of the controls the service provider has in place to ensure that any subservicer used by the service provider will be able to meet the Objectives.

Second, the institution must require its service providers, by contract, to implement appropriate measures designed to meet the Objectives. This provision does not require a service provider to have a security program in place that complies with each paragraph of the Guidelines. Because the focus is on compliance with the Objectives, there is some flexibility for a service provider's information security measures to differ from the program that the contracting financial institution implements. The precise terms and language of service contracts are left to the parties involved.

Third, depending on the risk assessment, the

institution may need to monitor its service providers to confirm that they have satisfied their contractual obligations to meet the Objectives. This monitoring should include reviews and evaluations of service providers, such as audits or summaries of test results. Monitoring does not necessarily require on-site inspections, but can instead be accomplished, for example, through the periodic review of the service provider's associated audits, summaries of test results, or equivalent measures of the service provider. Institutions should arrange to have these materials for review through contracts or other agreements.

As a caveat, a financial institution need only monitor its outsourcing arrangements if such oversight is indicated by the institution's own risk assessment. For example, where service providers are financial institutions who are already subject to the Guidelines, or are otherwise subject to other legal and professional standards that require them to safeguard the institution's customer and consumer information, then the institution may take these factors into account.

2.8 Adjusting the Program

In addition to monitoring and evaluating its information security program, each institution must continually adjust the program in light of changing circumstances. Adjustments to the program may be based on relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and changes to an institution's business arrangements (such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems). Any adjustment should involve a preliminary analysis of risks to customer information posed by new technology *before* a financial institution adopts the technology in order to determine whether a security program remains adequate in light of the new risks presented.

2.9 Reporting to the Board

At least once a year, it is required that the board be apprised of the overall status of the institution's information security program and its compliance with the Guidelines. The report should include "material" matters related to the program, such as: risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management responses, and recommendations for any changes to the program.

Although reporting to the board must occur at least annually, the Guidelines state that management of financial institutions with more complex information systems may find it necessary to provide information to the board on a more frequent basis. Similarly, more frequent reporting will be appropriate whenever a material event affecting the system occurs or a material modification is made to the system.

APPENDIX C – HIPAA SECURITY RULE – REQUIRED AND ADDRESSABLE SAFEGUARDS

Appendix A to Subpart C of Part 164—Security Standards: Matrix (1)

Standards	*Sections*	*Implementation Specifications (R)= Required, (A)= Addressable*
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement (R)

Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

APPENDIX D – RECENT FTC ENFORCEMENT ACTIONS FOR FAILING TO PROTECT CONSUMER PERSONAL INFORMATION

CASE SUMMARIES

A. CVS Caremark (Feb. 18, 2009)

According to the FTC's complaint, CVS Caremark (CVS) operates the largest pharmacy chain in the United States with more than 6,300 retail stores in addition to online and mail-order pharmacy businesses. The FTC began its investigation into CVS after it was reported that CVS pharmacies were throwing trash into open dumpsters with patient information visible and easily accessible.

The FTC's complaint alleged that CVS (1) failed to implement procedures for handling customer and employee personal information, most notably failing to implement a procedure for safely disposing of customer and employee personal information, (2) failed to adequately train employees with regard to the security of customer and employee personal information, (3) failed to assess its compliance with its own regulations regarding the secure disposal of personal information and (4) failed to attempt to discover and remedy the risks to the security of its customer and employee personal information.

The proposed settlement order requires that CVS establish, implement and maintain a comprehensive information security program designed to protect the security, confidentiality and integrity of the personal information it collects from consumers and employees. CVS is also required to obtain, every two years for the next twenty years, an audit from a qualified, independent, third-party professional to ensure that CVS's security program meets the standards of the order. The proposed settlement order also requires that CVS be subject to standard record-keeping and

reporting provisions to allow the FTC to monitor compliance and bars CVS from making future misrepresentations of the company's security practices.[110]

B. Genica Corporation (Feb. 5, 2009)

According to the FTC's complaint, Genica Corporation (Genica) is the parent company of Compgeeks.com (Compgeeks), which operates the website www.geeks.com. Compgeeks provides online services to consumers to authorize their online credit card purchases. Compgeeks collects sensitive consumer information, including the name, email address, address, telephone number and credit card information of consumers. Genica and Compgeeks stated that they took reasonable and appropriate measures to protect personal information from unauthorized access, with their privacy policy stating in part, "We use secure technology, privacy protection controls, and restrictions on employee access in order to safeguard your information." From about January 2007 to about June 2007, computer hackers accessed Genica's system and the consumer information stored therein.

The FTC complaint alleges that Genica (1) stored consumer information as unencrypted text on its computer network, (2) failed to sufficiently assess whether its applications and networks were susceptible to reasonably foreseeable attacks, and (3) failed to implement readily available and cost-effective security measures to defend against these attacks.

The settlement bars Genica from making deceptive claims regarding the security of its network and requires that Genica maintain a comprehensive information-security program that includes administrative, technical, and physical safeguards. The settlement also requires that Genica obtain, every other year for ten years, an audit from a qualified, independent, third-party professional to ensure that its

security program meets the standards of the order. Lastly, it requires that Genica be subject to standard record-keeping and reporting provisions to allow the FTC to monitor Genica's compliance with the settlement.[111]

C. Premier Capital Lending, Inc. (Nov. 6, 2008)

According to the FTC's complaint, Premier Capital Lending, Inc. is a mortgage lender. In connection with evaluating consumer applications for mortgage loans, Premier Capital Lending obtains consumer reports from a consumer reporting agency. Premier Capital Lending has an account with the consumer reporting agency and creates separate employee accounts which are used to obtain and store the consumer reports. Each employee account stores the name, address and full social security number that was used to obtain the reports along with the reports themselves for ninety days. The administrator of the consumer reporting account created an employee account for a home seller, who was located elsewhere in the state. This employee account enabled the home seller to access consumer reports of prospective buyers, and then refer them to Premier Capital Lending for a mortgage. No one from Premier Capital Lending visited the seller's workplace or audited the seller's computer.

Approximately four months later the security of the seller's computer was compromised and the hacker used the seller's consumer report account to request three hundred and seventeen new consumer reports for individuals that were not customers of Premier Capital Lending or the seller. During this time the hacker also had access to eighty-three reports generated by the seller's queries. Premier Capital Lending learned of the breach and notified the three hundred and seventeen individuals. Despite the fact that Premier Capital Lending could easily determine that the hacker also had access to the other eighty-three reports, Premier Capital

Lending did not send notice to the affected individuals until more than a year later.

The FTC alleged that Premier Capital Lending: (1) failed to provide reasonable and appropriate security for consumers' personal information because it failed to (a) assess the risk, (b) implement reasonable steps to address those risks, (c) reasonably review the consumer account access and (d) properly assess the scope of the breached information; (2) violated the safeguards rule, which requires that financial institutions develop procedures to protect customer information; and (3) violated the privacy rule, which requires that financial institutions provide a clear notice of the institution's policy and procedures to protect customer information, by disseminating a privacy policy that it did not follow.

The consent order requires that Premier Capital Lending establish, implement and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality and integrity of consumers' personal information. The settlement also requires Premier Capital Lending to obtain, every two years for the next twenty years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order.[112]

D. Reed Elsevier, Inc. (Mar. 27, 2008)

According to the FTC's complaint, Reed Elsevier, Inc., which owns LexisNexis, provides a series of verification products that allow customers to locate assets and people, authenticate identities and verify credentials. In order to provide this service, Reed Elsevier collects and aggregates information about millions of consumers and businesses from both public and non-public sources and makes this information available to its customers through websites. This information includes information from

consumer reporting agencies, including social security numbers.

The FTC alleged that Reed Elsevier failed to (1) provide reasonable and appropriate security to prevent unauthorized access to sensitive consumer information; and (2) failed to establish or implement reasonable policies and procedures governing the user credentials, including:

- Failing to establish strong enough passwords;
- Permitting the use of shared user credentials;
- Failing to require passwords to be changed;
- Failing to lock out accounts after unsuccessful login attempts;
- Permitting users to store their passwords in an insecure format;
- Failing to require that information containing sensitive information be encrypted;
- Failing to confirm the identify of new customers;
- Failing to adequately assess vulnerabilities in the technology infrastructure;
- Failing to implement simple, low-cost and readily available defenses.

The settlement requires Reed Elsevier to implement and maintain a comprehensive information-security program reasonably designed to protect the security, confidentiality and integrity of information collected from or about consumers made available through any information product

or service of LexisNexis. It must also include administrative, technical and physical safeguards. The settlement also requires the company to obtain, every two years for the next twenty years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order.[113]

E. TJX (Mar. 27, 2008)

According to the FTC's complaint, TJX is a an off-price retailer selling apparel and home fashions in over 2,500 stores worldwide, including, but not limited to, T.J. Maxx, Marshalls, A.J. Wright, Bob's Stores and HomeGoods stores in the United States; Winners and HomeSense in Canada; and T.J. Maxx stores in the United Kingdom, Ireland and Germany. Consumers may pay for purchases at these stores with credit and debit cards, cash or personal checks. TJX operates computer networks used to process sales transactions and provides wireless access to the networks for wireless devices, such as devices for marking down prices. In addition, the network is used to collect personal information from consumers to obtain authorization for payment card purchases, verify personal checks and process merchandise returned without receipts. Among other things, it collects: (1) account number, expiration date and an electronic security code for payment card authorization; (2) bank routing, account and check numbers and, in some instances, driver's license number and date of birth for personal check verification; and (3) name, address, and drivers' license, military or state identification numbers.

The FTC alleged that TJX failed to (1) provide reasonable and appropriate security for sensitive consumer information stored on its computer network; (2) restrict access to its network to authorized users; (3) require network administrators and other users to use strong passwords; and (4) encrypt stored authorization requests and personal information on its in-store and corporate networks, instead

using clear text. As a result of these failures, an intruder connected to the networks, installed hacker tools, found personal information stored in clear text, and downloaded it over the Internet to remote computers. Furthermore, an intruder periodically intercepted payment card authorization requests in transit from in-store networks to the central corporate network and transmitted the files over the Internet to remote computers.

The consent order requires the TJX to implement and maintain a comprehensive information-security program reasonably designed to protect the security, confidentiality and integrity of personal information collected from or about consumers. It must also include administrative, technical and physical safeguards. The settlement also requires the company to obtain, every two years for the next twenty years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order. [114]

F. ValueClick (Mar. 17, 2008)

According to the FTC's complaint, ValueClick, through its subsidiary and co-defendant Hi-Speed Media, operates its lead generation business which connects consumers to advertisers. It advertises and markets offers through email and Web-based mediums. In connection with promotions and advertisements on its websites and in its email, ValueClick has offered consumers free merchandise, such as iPods, laptop computers and Visa gift cards. There is no clear and conspicuous disclosure that to obtain the promised free merchandise one must incur expenses or other obligations. Through another subsidiary, ValueClick also sold and marketed consumer products through its sites which required personal information stored on its databases. Its privacy policy states, "At our site you can be assured that your Personally Identifiable Information is secure, consistent with current industry standards. . . . We encrypt your

Personally Identifiable Information and thereby prevent unauthorized parties from viewing such information when it is transmitted to us."

The FTC alleged that ValueClick violated the (i) FTC Act when it failed to disclose or inadequately disclosed material information that its advertised offers were with cost or obligation; (ii) FTC Act privacy rule by providing customers with a privacy policy that contained false or misleading statements about encryption; (iii) FTC Act by falsely representing to consumers that it implements reasonable and appropriate measures to protect personal information and (iv) CAN-SPAM Act by transmitting commercial email messages with misleading headings.

The judgment requires ValueClick to disclose consumer obligations related to offers, prohibits it from transmitting commercial email messages with misleading headings and misrepresenting security standards. In addition, ValueClick was fined $2.9M. It also requires the company to implement and maintain a comprehensive information-security program that includes administrative, technical and physical safeguards. The judgment also requires the company to obtain, every two years for the next twenty years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order.[115]

G. Goal Financial (Mar. 4, 2008)

According to the FTC's complaint, Goal Financial, LLC, collects personal information from applicants in the course of providing student loans and related services. As a result of security failures, employees transferred more than 7,000 files with consumer information to third parties without authorization, and one employee sold to the public surplus hard drives that contained, in clear text, information about 34,000 consumers. [116]

The FTC alleged that Goal Financial violated (i) the safeguards rule by failing to: adequately assess the risks to consumers' personal information, adequately restrict access to this information to authorized employees, implement a comprehensive information security program, provide adequate employee training, and, in some instances, contractually require third-party service providers to protect the information; (ii) the privacy rule by providing customers with a privacy policy that contained false or misleading statements, and (iii) the FTC Act by falsely representing to consumers that it implements reasonable and appropriate measures to protect personal information.

The consent order bars Goal Financial from future data security misrepresentations and requires the company to implement and maintain a comprehensive information-security program that includes administrative, technical and physical safeguards. The settlement also requires the company to obtain, every two years for the next ten years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order.

H. Life is good (Jan. 17, 2008)

Life is good designs and sells retail apparel and accessories and operates the Web site, www.lifeisgood.com. According to the FTC's complaint, through its Web site, Life is good has collected sensitive consumer information, including names, addresses, credit card numbers, credit card expiration dates and credit card security codes. Its privacy policy claimed, "We are committed to maintaining our customers' privacy. We collect and store information you share with us – name, address, credit card and phone numbers along with information about products and services you request. All information is kept in a secure file and is used to tailor our communications with you."

The FTC alleged that Life is good failed to provide reasonable and appropriate security for the sensitive consumer information stored on its computer network.[117] The FTC alleges that, as a result of these failures, a hacker was able to use SQL injection attacks on Life is good's Web site to access the credit card numbers, expiration dates and security codes of thousands of consumers.

The settlement requires the company to establish and maintain a comprehensive security program reasonably designed to protect the security, confidentiality and integrity of personal information it collects from consumers.[118] Specifically, Life is good must:

- Designate an employee or employees to coordinate the information security program.
- Identify internal and external risks to the security and confidentiality of personal information and assess the safeguards already in place.
- Design and implement safeguards to control the risks identified in the risk assessment and monitor their effectiveness.
- Develop reasonable steps to select and oversee service providers that handle the personal information of Life is good customers.
- Evaluate and adjust its information-security program to reflect the results of monitoring, any material changes to the company's operations or other circumstances that may impact the effectiveness of its security program.

The settlement requires Life is good to retain an

independent, third-party security auditor to assess its security program on a biennial basis for the next twenty years.

I. American United Mortgage Company (Dec. 18, 2007)

The FTC's complaint alleged that American United Mortgage Company ("American United") violated the disposal, safeguards and privacy rules by failing to properly dispose of credit reports or information taken from credit reports, failing to develop or implement reasonable safeguards to protect customer information, and not providing customers with privacy notices.[119]

According to the FTC's complaint, the company engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers' personal information. For example, the company allegedly failed to implement reasonable policies and procedures requiring the proper disposal of consumers' personal information, including consumer reports; to take reasonable actions in disposing of such information; and to identify reasonably foreseeable internal and external risks to consumer information.

As a result of these failures, the complaint alleged, on multiple occasions American United documents containing consumers' personal information were found in and around a dumpster, near its office, that was unsecured and easily accessible to the public. The complaint also alleged that from July 1, 2001 until March 2006, the company failed to provide its customers with a privacy notice as required by the FTC's Privacy Rule.

The stipulated judgment and final order requires American United to pay a $50,000 civil penalty for violations of the Disposal Rule. This was the FTC's first enforcement action against a company for violating the Disposal Rule.

J. Guidance Software (Mar. 30, 2007)

Guidance is a company that provides software and training "that customers use to, among other things, investigate and respond to computer breaches and other security incidents."[120] Guidance collected and stored customer information such as credit card numbers, expiration dates and security codes, in addition to names, addresses, emails and telephone numbers.

Although Guidance employed SSL encryption, it (1) stored customer information in "clear readable text"; (2) did not adequately prepare for commonly known attacks, such as SQL injection attacks; (3) "stored in clear readable text network user credentials that facilitate[d] access to sensitive personal information on the network"; (4) did not use simple security measures to monitor and control connections between the network and the Internet; and (5) did not use "sufficient measures to detect unauthorized access to sensitive personal information."[121]

Like the earlier complaints, the FTC alleged that these practices led to security breaches and fraudulent activity. In addition, the FTC's complaint charged Guidance with falsely representing (on the Guidance website) that it had taken appropriate steps to safeguard customer information. In the final consent order, Guidance agreed to the FTC's standardized Security Program/Auditing/Compliance demands, and additionally agreed to "not misrepresent in any manner, expressly or by implication, the extent to which respondent maintains and protects the privacy, confidentiality, security, or integrity of any personal information collected from or about consumers."[122]

Another prominent difference between the Guidance Software Consent Decree and earlier orders was a requirement that Guidance take "reasonable steps" to ensure

that any of its service providers handling customer information maintain a similar commitment to information security.[123] Specifically, Guidance consented to "the development and use of reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from [Guidance], requiring service providers by contract to implement and maintain appropriate safeguards, and monitoring their safeguarding of personal information."[124] Guidance Software's responsibility for data breaches by service providers further increases its potential liability for any future disclosure of customer information.

K. CardSystems Solutions (Sept. 5, 2006)

CardSystems Solutions acts as a middle-man between merchants and card-issuing banks in authorizing credit and debit card purchases. "CardSystems collected information from the magnetic strip of [each card used], including the card number, expiration date, and other data." CardSystems (1) unnecessarily stored this information; (2) used weak passwords to protect access to its network and the files containing the information; (3) "did not use readily available security measures to limit access between computers on its network and between its computers and the Internet"; (4) "did not adequately assess the vulnerability of its computer network to commonly known or reasonably foreseeable attacks, including 'Structured Query Language' injection attacks"; and (5) "did not implement simple, low-cost, and readily available defenses to such attacks." As in the previous cases, these practices were alleged to have resulted in millions of dollars in fraudulent purchases.[125]

L. DSW (Mar. 7, 2006)

DSW is a large shoe retailer that collected information from the magnetic strip of every credit card used to make a purchase. Additionally, DSW collected information from customers paying by check, including

account, routing, check, and driver's license numbers. For both credit and check purchases, information was wirelessly transmitted to an in-store computer network, which then transmitted the information to banks and check processors.[126]

DSW (1) failed to limit wireless access to these in-store networks, and (2) failed to limit access between and among individual in-store and corporate networks. Like BJ's (described in Section N below), it (3) stored information it no longer needed in (4) unencrypted files protected only by a commonly known user ID and password. Also like BJ's, DSW (5) failed to employ sufficient measures to detect unauthorized access. As a result of these alleged practices, the company's exposure for breach related losses were estimated at between $6.5 to $9.5 million dollars.[127]

M. ChoicePoint (Jan. 26, 2006)

ChoicePoint is an information broker that obtains and sells the personal information of consumers, including their names, Social Security numbers, birth dates, employment information, and credit histories to more than 50,000 businesses.

The FTC alleged that ChoicePoint (1) failed to maintain reasonable procedures to screen prospective subscribers, and turned over consumers' sensitive personal information to subscribers whose applications were suspicious; and (2) violated the FTC Act by making false and misleading statements about its privacy policies. As a result, about 800 people became victims of identity theft when ChoicePoint sold their personal information to identity thieves who posed as legitimate business customers.

ChoicePoint was ordered to pay $10 million in civil penalties and to provide $5 million for consumer redress. It was barred from furnishing consumer reports to people who do not have a permissible purpose to receive them and

ordered to verify the identity of businesses that apply to receive consumer reports. The order also required ChoicePoint to establish, implement and maintain a comprehensive information security program designed to protect the security, confidentiality and integrity of the personal information it collects from or about consumers. It also required ChoicePoint to obtain an audit every two years for the next twenty years.[128]

N. BJ's Wholesale Club (Sept. 20, 2005)

BJ's is a large wholesale corporation operating hundreds of warehouses and gas stations throughout the east coast. Whenever a customer purchased goods with a credit or debit card, BJ's collected information from the card's magnetic strip that was relayed from the store network to a central datacenter network, which further communicated with the external network of the card-issuing bank.[129]

BJ's (1) failed to encrypt this information during storage or transmission; (2) stored it for longer than needed in violation of bank security rules; (3) used commonly known default user IDs and passwords to protect the information; (4) failed to use available security measures to prevent wireless access to its networks; and (5) failed to detect unauthorized access or conduct security investigations. As a result of these lax security measures, cards used at BJ's were counterfeited and used to make approximately $13 million dollars in fraudulent purchases.[130]

APPENDIX E – RECENT LITIGATION FOR FAILING TO PROTECT CONSUMER INFORMATION

CASE SUMMARIES

1. *Kahle v. Litton Loan Servicing L.P.*

Litton is a mortgage loan service provider located in Houston, Texas with facilities in other cities, including Atlanta, Georgia.[131] Computer equipment was stolen from the Atlanta office, including six unmarked hard drives, with personal information of 229,502 former customers of Provident Bank, who owned the loans serviced by Litton. Litton provided notice to the affected customers.

On behalf of a class, plaintiff brought claims for negligence, invasion of privacy, fraud and violation of consumer protection statutes. Litton moved for summary judgment arguing that the plaintiff had no damages.

On May 16, 2007 the U.S. District Court for the Southern District of Ohio held that the cost of enrolling in a credit protection program due to a fear of identity theft did not constitute a sufficient damage to support a negligence claim arising from a data breach incident. The decision follows the general rule that the risk of future injury is not a sufficient harm to support a negligence claim against a financial institution.

2. *Pisciotta v. Old Nat'l Bancorp*

In 2002 and 2004, plaintiffs submitted loan application information to ONB through the bank Web site. NCR, the Web hosting facility, reported a security breach in 2005. The nature of the breach is not reported, but after reviewing sealed materials in chambers, the court noted that the unauthorized access was "sophisticated, intentional and malicious."[132] ONB notified its customers of the breach.

Plaintiffs claimed negligence and breach of implied contract, on behalf of a class of tens of thousands of ONB site users. ONB moved for judgment on the pleadings, arguing that plaintiffs' negligence and contract claims failed

because they had no damages.

The district court granted ONB's motion and on Aug. 23, 2007, the U.S. Court of Appeals for the Seventh Circuit affirmed the decision. The court held that costs for credit monitoring, to guard against some future, anticipated harm, are not compensable injuries under Indiana law.

3. *In re TJX Cos. Retail Security Breach Litig.*

On September 21, 2007 TJX Companies Inc. filed a proposed settlement agreement in the U.S. District Court for the District of Massachusetts to resolve consolidated class action litigation filed by consumers in the United States, Puerto Rico, and Canada in connection with hacking incidents that exposed personal and financial information on at least 46 million credit and debit cards.[133]

The settlement provides for different benefits to different subclasses. Approximately 450,000 "unreceipted return customers" whose driver's license information was copied and exposed may receive reimbursement for the cost of new driver's licenses and credit monitoring costs. Members of the larger class that purchased at TJX stores can get vouchers totaling up to a capped $7 million payout. A store-wide 15% sale in 2008 is also planned. The settlement provides for $6.65 million in attorneys' fees and costs.

The agreement did not settle class action claims filed by payment card-issuing banks seeking reimbursement of their costs, including the cost of replacing cards affected by the breach and covering fraudulent purchases. The banks alleged negligence, breach of contract and negligence *per se*. TJX settled with the banks for $40 million in December 2007.

[1] For example, the European Community enacted its Data Protection Directive 95/46/EC in 1995, and subsequent to that the EU member states enacted their own implementing legislation. The EU Data Protection Directive and member state legislation impose many regulations on the collection, processing, use, disclosure and transfer of personal information.

[2] In the U.S., nonpublic personal information for consumers and customers of financial institutions is regulated under the Gramm-Leach-Bliley Act of 1999, and associated regulations, and protected health information processed by covered entities is regulated under the Health Insurance Portability and Accountability Act (HIPAA) and associated regulations.

[3] As of May 25, 2009, 44 states and the District of Columbia have enacted some form of database breach notification law. In addition, the FTC has been active in enforcement actions from violations of privacy notices to charges and resulting settlements with Goal Financial, Life is Good, American United Mortgage Company, BJ's Wholesale Club, Inc. and DSW, Inc. for failing to protect customer information.

[4] Survey, 2006 CSI/FBI Computer Crime and Security Survey, p.10. (available at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf).

[5] For a discussion of the effects of privacy breaches on stock prices, see James DeLuccia IV, "Do Data Leaks Really Affect Share Prices?" (http://pcidss.wordpress.com/2006/10/26/do-data-leaks-really-affect-share-prices-by-james-deluccia-iv/).

[6] Concern for privacy issues is not just about having a privacy notice on the company Web site. With respect to employees, your business faces many privacy issues regarding personnel files, medical and insurance information, performance data, portals, e-learning facilities, and e-mail and Internet use, to name a few. If your business collects information about customers, whether in a consumer or a business context, then your business has privacy issues regarding the collection, use, disclosure and transfer of that data. If your business operates abroad, many other countries have privacy laws that affect your data. If your business shares data with third parties, whether as service providers, alliance partners or otherwise, then your business needs to be concerned about the privacy practices of these third parties, and how they can impact your business.

[7] Privacy Rights Clearinghouse at www.privacyrights.org/ar/ChronDataBreaches.htm.

[8] The FTC enforcement orders generally define personal information as follows: "Personal Information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical

address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number, and check number; (h) a driver's license number; or (i) any other information from or about an individual consumer that is combined with (a) through (h) above.

[9] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq*.; Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.*

[10] Health Insurance Portability and Accountability Act, 42 U.S.C. §§ 1320 *et seq.*

[11] 15 U.S.C. §§ 6501 *et seq*.

[12] *See* Consent Decree and Order for Civil Penalties, Imbee.com (Jan. 30, 2008)(available at http://www.ftc.gov/os/caselist/0723082/080730cons.pdf); Consent Decree and Order for Civil Penalties, Xanga (Sept. 7, 2006)(available at http://www.ftc.gov/os/caselist/0623073/xangaconsentdecree.pdf).

[13] Examples of federal statutes regulating the use and collection of personal information in the public sector include the Privacy Act, 5 U.S.C. § 552a, and the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541 *et seq.*

[14] 15 U.S.C. § 1681w.

[15] 15 U.S.C. §§ 1692 *et seq.*

[16] Pub. Law 107-56.

[17] 12 U.S.C. §§ 3401 *et seq.*

[18] Concurring Statement of Commissioner Jon Leibowitz, FTC Staff Report "Self-Regulatory Principles for Online Behavioral Advertising" (Feb. 2009)(available at http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf).

[19] *See, e.g.*, California Office of Information Security and Privacy Protection (www.privacy.ca.gov).

[20] *See, e.g.*, An Act Concerning the Confidentiality of Social Security Numbers, 2008 Conn. Pub. Acts No. 08-167.

[21] *See, e.g.*, Cal. Bus. & Prof. Code § 17200; Mass. Gen. L. Chap. 167, § 2A.

[22] 15 U.S.C. § 45 (2007).

[23] 201 Mass. Code Regs. § 17.00 (2008).

[24] The New York Consumer Protection Board's Business Privacy Guide is available at http://www.consumer.state.ny.us/pdf/the_new_york_business_guide_to_privacy.pdf.

[25] *See Guin v. Brazos Higher Education Service*, 2006 U.S. Dist. Lexis 4846 (D.Minn. 2006) (court refused to hold that encryption was a required legal standard, as contrasted with recent FTC consent decrees), discussed herein, where the FTC found liability for failure to encrypt consumer information.

[26] Many information security standards are available that discuss frameworks and programs for information security compliance. For example, there is ISO/IEC 27001, ISO/IEC 27002, NIST Special Publication 800-14, known as the Generally Accepted Principles and Practices for Securing Information Technology Systems, and the Payment Card Industry Data Security Standards. Many of these standards are criticized, however, as lacking in specific recommendations and details as to how to accomplish the general principles they set forth.

[27] *See,* Cal. Civ. Code 1798.82 and 1798.29.

[28] *See* State Security Breach Notification Laws (May 26, 2009)(available at http://www.ncsl.org/Default.aspx?TabId=13489).

[29] *See, e.g.*, Nev. Rev. Stat. § 603A.220 (2007).

[30] *See Id.*

[31] *Id.*

[32] Nev. Rev. Stat. § 597.970.

[33] 201 Mass. Code Regs. § 17.00 (2008).

[34] *Id.*

[35] 201 Mass. Code Regs. §§ 17.03, 17.04 (2008).

[36] A.B. 211, 2009 Leg., Reg. Sess. (Cal. 2009).

[37] *Id.*

[38] S.B. 541, 2009 Leg., Reg. Sess. (Cal. 2009).

[39] Press Release, State of New York, Office of the Attorney General, Cuomo Obtains First Agreement For Violation of Security Breach Notification law, (Apr. 26, 2007)(available at http://www.oag.state.ny.us/media_center/2007/apr/apr26a_07.html).

[40] N.Y. State Info. Sec. Breach and Notification Act (2005) (amending N.Y. Gen. Bus. § 899-aa (2008) and N.Y. State Tech. § 208 (2008)).

[41] Press Release, State of New York, Office of the Attorney General, Cuomo Obtains First Agreement For Violation of Security Breach Notification law, (Apr. 26, 2007)(available at http://www.oag.state.ny.us/media_center/2007/apr/apr26a_07.html).

[42] *Id*.

[43] The New York Consumer Protection Board's Business Privacy Guide, *supra* note 24.

[44] *Id*.

[45] *Id*.

[46] A.B. 2270, 213th Leg., Reg. Sess. (N.J. 2008).

[47] H.B. 100, 95th Gen. Assem., Reg. Sess. (Mo. 2009).

[48] *Id.*

[49] These sections also require the Securities and Exchange Commission ("SEC") to establish appropriate standards for brokers, dealers, investment companies and investment advisers. The SEC issued initial guidance regarding the appropriate standards as part of Regulation S-P which implemented GLB. 16 C.F.R. Part 248.

[50] The Guidelines began as a joint effort by the Federal Banking Agencies to implement sections 501 and 505(b) of GLB. The Guidelines were originally published as the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" in early 2001. In late

2004, the Federal Banking Agencies, the FTC and the SEC issued final rules entitled "Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003." *See* 69 Fed. Reg. 68690 (2004) (FTC); 69 Fed. Reg. 77610 (2004) (Federal Banking Agencies); 69 Fed. Reg. 71322 (2004) (SEC). The Federal Banking Agencies' final rule amended the Guidelines by: (i) adding a definition of "consumer information," including illustrations of information covered by the term; (ii) adding an objective regarding the proper disposal of both customer information and consumer information; and (iii) adding a provision that requires a financial institution to implement appropriate measures to properly dispose of customer information and consumer information in accordance with each of the stated procedures for disposing of information. Additionally, the final rule renamed the Guidelines to their current title, in order to make clear that the Guidelines now encompass the disposal of consumer information as well as customer information.

[51] The Small-Entity Compliance Guide is available at http://www.federalreserve.gov/Regulations/cg/infosec.htm.

[52] 70 Fed. Reg. 15736 (2005).

[53] 45 C.F.R. § 160.103.

[54] 45 C.F.R. Part 164.

[55] 45 C.F.R. § 160.103.

[56] The Office of Civil Right of HHS provided a sample Business Associate Agreement (http://www.hhs.gov/ocr/hipaa/contractprov.html).

[57] 45 C.F.R. § 164.504.

[58] 45 C.F.R. Parts 160 and 164.

[59] American Recovery and Reinvestment Act of 2009, H. R. 1, 111th Cong. § 13401(b) (2009) (enacted).

[60] H. R. 1 § 13401(a) (enacted); 45 C.F.R. Part 164.

[61] H. R. 1 § 13404(a) (enacted).

[62] *Id.*

[63] H. R. 1 § 13402 (enacted).

[64] H. R. 1 §§ 13401(a) and 13402(d) (enacted).

[65] H. R. 1 § 13402(h)(2) (enacted).

[66] H. R. 1 § 13410(e) (enacted).

[67] H. R. 1 § 13410(d) (enacted).

[68] *Id.*

[69] H. R. 1 § 13410(b) (enacted).

[70] Press Release, U.S. Department of Health & Human Services, HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information (July 17, 2008)(available at http://www.hhs.gov/news/press/2008pres/07/20080717a.html).

[71] *Id.*

[72] *Id.*

[73] Pub. L. 107-204, Sections 302 and 404.

[74] Consumer or personal information includes data such as first and last name, address, online contact information, telephone number, Social Security number, credit card information, "cookies," *etc*. *See, e.g.*, In the Matter of CVS Caremark Corporation, File No. 072-3119, at 3 (Feb. 18, 2009) (agreement containing consent order) (available at

http://www.ftc.gov/os/caselist/0723119/090218cvsagree.pdf); In the Matter of Genica Corporation and Compgeeks.com, Docket No. C-4252, at 2 (Mar. 20, 2009) (decision and order) (available at http://www.ftc.gov/os/caselist/0823113/090320genicado.pdf); In the Matter of Premier Capital Lending, Inc., and Debra Stiles, Docket No. C-4241, at 2 (Dec. 16, 2008) (decision and order) (available at http://www.ftc.gov/os/caselist/0723004/081216pcldo.pdf); In the Matter of The TJX Companies, Inc., Docket No. C-4227, at 2 (Aug. 1, 2008) (decision and order) (available at http://www.ftc.gov/os/caselist/0723055/080801tjxdo.pdf); In the Matter of Reed Elsevier Inc. and Seisint, Inc., Docket No. C-4226, at 2 (Aug. 1, 2008) (decision and order) (available at http://www.ftc.gov/os/caselist/0523094/080801reeddo.pdf); *U.S. v. ValueClick, Inc., Hi-Speed Media, Inc., and E-Babylon, Inc.*, File Nos. 072-3111 and 072-3158, at 5 (Mar. 17, 2008) (stipulated final judgment for civil penalties and permanent injunctive relief) (available at http://www.ftc.gov/os/caselist/0723111/080317judgment.pdf); In the Matter of Goal Financial, LLC, File No. 072-3013, at 2 (Mar. 4, 2008) (agreement containing consent order) (available at http://www.ftc.gov/os/caselist/0723013/080304agreement.pdf); In the Matter of Life is good, Inc., and Life is good Retail, Inc., File No. 072-3046, at 2 (Jan. 17, 2008) (agreement containing consent order) (available at http://www.ftc.gov/os/caselist/0723046/080117agreement.pdf); In the Matter of Guidance Software, Inc., Docket No. C-4187, at 2 (Apr. 3, 2007) (decision and order) (available at http://www.ftc.gov/os/caselist/0623057/0623057do.pdf); In the Matter of CardSystems Solutions, Inc., Docket No. C-4168, at 2 (Sept. 8, 2006) (decision and order) (available at http://www.ftc.gov/os/caselist/0523148/0523148CardSystemsdo.pdf); In the Matter of DSW Inc., Docket No. C-4157, at 2 (Mar. 7, 2006) (decision and order) (available at http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWDecisionandOrder.pdf); In the Matter of BJ's Wholesale Club, Inc., Docket No. C-4148, at 2 (Sept. 20, 2005) (decision and order) (available at http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf).

[75] *Identity Theft: FTC Won't Enforce Red Flags Until May '09; Banks Still Must Comply With Rules by Nov. 1*, 7 PVLR (BNA) 1533 (Oct. 27, 2008).

[76] *See* FTC Press Release, "FTC Will Grant Six-Month Delay of Enforcement of 'Red Flags' Rule Requiring Creditors and Financial Institutions to Have Identity Theft Prevention Programs" (Oct. 22, 2008) (available at http://www.ftc.gov/opa/2008/10/redflags.shtm).

[77] 15 U.S.C. § 45 (2007).

[78] Analysis of Proposed Consent Order to Aid Public Comment, DSW Inc., 70 Fed. Reg. 73474 (2005).

[79] FTC Press Release, "BJ's Wholesale Club Settles FTC Charges" (June 16, 2005) (available at http://www.ftc.gov/opa/2005/06/bjswholesale.shtm).

[80] *See* FTC Press Release, "Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data" (Mar. 27, 2008) (available at http://www.ftc.gov/opa/2008/03/datasec.shtm); FTC Press Release, "Online Apparel Life is Good Retailer Settles FTC Charges" (Jan, 17, 2008) (available at http://www.ftc.gov/opa/2008/01/lig.shtm); FTC Press Release "Guidance Software Settles FTC Charges" (Nov. 16, 2006) (available at http://www.ftc.gov/opa/2006/11/guidance.shtm); FTC Press Release, "CardSystems Solutions Settles FTC Charges" (Feb. 23, 2006) (available at http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm); FTC Press Release, "DSW Inc. Settles FTC Charges" (Dec. 1, 2005) (available at http://www.ftc.gov/opa/2005/12/dsw.shtm); FTC Press Release, "BJ's Wholesale Club Settles FTC Charges," *supra* note 79.

[81] *See* FTC Press Release, "Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data," *supra* note 80; FTC Press Release, "Online Apparel Life is Good Retailer Settles FTC Charges," *supra* note 80; FTC Press Release "Guidance Software Settles FTC Charges," *supra* note 80; FTC Press Release, "CardSystems Solutions Settles FTC Charges," *supra* note 80; FTC Press Release, "DSW Inc. Settles FTC Charges," *supra* note 80; FTC Press Release, "BJ's Wholesale Club Settles FTC Charges," *supra* note 79.

[82] *See* FTC Press Release, "Online Apparel Life is Good Retailer Settles FTC Charges," *supra* note 80; Analysis of Proposed Consent Order to Aid Public Comment, 73 Fed. Reg. 4231 (2008); Analysis of Proposed Consent Order to Aid Public Comment, DSW Inc., 70 Fed. Reg. 73474 (2005).

[83] *See* FTC Press Release, "Consumer Electronics Company Agrees to Settle Data Security Charges; Breach Compromised Data of Hundreds of Consumers" (Feb. 5, 2009) (available at http://www.ftc.gov/opa/2009/02/compgeeks.shtm); FTC Press Release, "Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data," *supra* note 80; FTC Press Release, "ValueClick to Pay $2.9 Million to Settle FTC Charges" (Mar. 17, 2008) (available at http://www.ftc.gov/opa/2008/03/vc.shtm); FTC Press Release, "Online Apparel Life is Good Retailer Settles FTC Charges," *supra* note 80; FTC Press Release, "CardSystems Solutions Settles FTC Charges," *supra* note 80; FTC Press Release, "Guidance Software Settles FTC Charges," *supra* note 80.

[84] *See* FTC Press Release, "Consumer Electronics Company Agrees to Settle Data Security Charges; Breach Compromised Data of Hundreds of Consumers," *supra* note 83; FTC Press Release, "Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data," *supra* note 80; FTC Press Release, "ValueClick to Pay $2.9 Million to Settle FTC Charges," *supra* note 83;

FTC Press Release, "Online Apparel Life is Good Retailer Settles FTC Charges," *supra* note 80; FTC Press Release, "CardSystems Solutions Settles FTC Charges," *supra* note 80; FTC Press Release, "Guidance Software Settles FTC Charges," *supra* note 80.

[85] *See* FTC Press Release, "CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations" (Feb. 18, 2009) (available at http://www.ftc.gov/opa/2009/02/cvs.shtm).

[86] CVS Caremark Corporation (agreement containing consent order), *supra* note 74, at 3; Genica Corporation and Compgeeks.com (decision and order), *supra* note 74, at 3; Premier Capital Lending and Debra Stiles (decision and order), *supra* note 74, at 3; The TJX Companies (decision and order), *supra* note 74, at 2; Reed Elsevier and Seisint (decision and order), *supra* note 74, at 3; *ValueClick* (stipulated final judgment for civil penalties and permanent injunctive relief), *supra* note 74, at 9; Goal Financial (agreement containing consent order), *supra* note 74, at 4; Life is good (agreement containing consent order), *supra* note 74, at 4; BJ's (decision and order), *supra* note 74, at 2; DSW (decision and order), *supra* note 74, at 2; CardSystems Solutions (decision and order), *supra* note 74, at 3; Guidance Software (decision and order), *supra* note 74, at 3.

[87] CVS Caremark Corporation (agreement containing consent order), *supra* note 74, at 4; Genica Corporation and Compgeeks.com (decision and order), *supra* note 74, at 4; Premier Capital Lending and Debra Stiles (decision and order), *supra* note 74, at 4; The TJX Companies (decision and order), *supra* note 74, at 3; Reed Elsevier and Seisint (decision and order), *supra* note 74, at 4; *ValueClick* (stipulated final judgment for civil penalties and permanent injunctive relief), *supra* note 74, at 11; Goal Financial (agreement containing consent order), *supra* note 74, at 4; Life is good (agreement containing consent order), *supra* note 74, at 4; BJ's (decision and order), *supra* note 74, at 3; DSW (decision and order), *supra* note 74, at 3; CardSystems Solutions (decision and order), *supra* note 74, at 3-4; Guidance Software (decision and order), *supra* note 74, at 3-4.

[88] CVS Caremark Corporation (agreement containing consent order), *supra* note 74, at 5; Genica Corporation and Compgeeks.com (decision and order), *supra* note 74, at 5; Premier Capital Lending and Debra Stiles (decision and order), *supra* note 74, at 5; The TJX Companies (decision and order), *supra* note 74, at 4; Reed Elsevier and Seisint (decision and order), *supra* note 74, at 5; *ValueClick* (stipulated final judgment for civil penalties and permanent injunctive relief), *supra* note 74, at 13; Goal Financial (agreement containing consent order), *supra* note 74, at 5; Life is good (agreement containing consent order), *supra* note 74, at 5; BJ's (decision and order), *supra* note 74, at 4-5; DSW (decision and order), *supra* note 74, at 4-5; CardSystems Solutions (decision and order), *supra* note 74, at 4-5; Guidance Software (decision and order), *supra* note 74, at 4-5.

[89] CVS Caremark Corporation (agreement containing consent order), *supra* note 74, at 3; Genica Corporation and Compgeeks.com (decision and order), *supra* note 74, at 3; Premier Capital Lending and Debra Stiles (decision and order), *supra* note 74, at 3; The TJX Companies (decision and order), *supra* note 74, at 2; *ValueClick* (stipulated final judgment for civil penalties and permanent injunctive relief), *supra* note 74, at 10; Goal Financial (agreement containing consent order), *supra* note 74, at 3; Life is good (agreement containing consent order), *supra* note 74, at 3; BJ's (decision and order), *supra* note 74, at 2; DSW (decision and order), *supra* note 74, at 2; CardSystems Solutions (decision and order), *supra* note 74, at 3; Guidance Software (decision and order), *supra* note 74, at 3.

[90] CVS Caremark Corporation (agreement containing consent order), *supra* note 74, at 4; Genica Corporation and Compgeeks.com (decision and order), *supra* note 74, at 3; Premier Capital Lending and Debra Stiles (decision and order), *supra* note 74, at 3; The TJX Companies (decision and order), *supra* note 74, at 3; Reed Elsevier and Seisint (decision and order), *supra* note 74, at 3; *ValueClick* (stipulated final judgment for civil penalties and permanent injunctive relief), *supra* note 74, at 10; Goal Financial (agreement containing consent order), *supra* note 74, at 3; Life is good (agreement containing consent order), *supra* note 74, at 3; BJ's (decision and order), *supra* note 74, at 3; DSW (decision and order), *supra* note 74, at 3; CardSystems Solutions (decision and order), *supra* note 74, at 3; Guidance Software (decision and order), *supra* note 74, at 3.

[91] CVS Caremark Corporation (agreement containing consent order), *supra* note 74, at 4; Genica Corporation and Compgeeks.com (decision and order), *supra* note 74, at 3; Premier Capital Lending and Debra Stiles (decision and order), *supra* note 74, at 3; The TJX Companies (decision and order), *supra* note 74, at 3; Reed Elsevier and Seisint (decision and order), *supra* note 74, at 3; *ValueClick* (stipulated final judgment for civil penalties and permanent injunctive relief), *supra* note 74, at 10; Goal Financial (agreement containing consent order), *supra* note 74, at 3; Life is good (agreement containing consent order), *supra* note 74, at 3; BJ's (decision and order), *supra* note 74, at 3; DSW (decision and order), *supra* note 74, at 3; CardSystems Solutions (decision and order), *supra* note 74, at 3; Guidance Software (decision and order), *supra* note 74, at 3.

[92] CVS Caremark Corporation (agreement containing consent order), *supra* note 74, at 4; Genica Corporation and Compgeeks.com (decision and order), *supra* note 74, at 3; Premier Capital Lending and Debra Stiles (decision and order), *supra* note 74, at 3; The TJX Companies (decision and order), *supra* note 74, at 3; Reed Elsevier and Seisint (decision and order), *supra* note 74, at 4; *ValueClick* (stipulated final judgment for civil penalties and permanent injunctive relief), *supra* note 74, at 10; Goal Financial (agreement containing consent order), *supra* note 74, at 3; Life is good (agreement containing consent order), *supra* note 74, at 3; BJ's (decision and order), *supra* note 74, at 3; DSW (decision and order), *supra* note 74, at 3; CardSystems Solutions

(decision and order), *supra* note 74, at 3; Guidance Software (decision and order), *supra* note 74, at 3.

[93] CVS Caremark Corporation (agreement containing consent order), *supra* note 74, at 4; Genica Corporation and Compgeeks.com (decision and order), *supra* note 74, at 4; Premier Capital Lending and Debra Stiles (decision and order), *supra* note 74, at 4; The TJX Companies (decision and order), *supra* note 74, at 3; Reed Elsevier and Seisint (decision and order), *supra* note 74, at 4; *ValueClick* (stipulated final judgment for civil penalties and permanent injunctive relief), *supra* note 74, at 11; Goal Financial (agreement containing consent order), *supra* note 74, at 3; Life is good (agreement containing consent order), *supra* note 74, at 3; BJ's (decision and order), *supra* note 74, at 3; DSW (decision and order), *supra* note 74, at 3; CardSystems Solutions (decision and order), *supra* note 74, at 3; Guidance Software (decision and order), *supra* note 74, at 3.

[94] 698 A.2d 959 (Del. Ch. 1996).

[95] 2005 Mich. App. LEXIS 353 (Mich. App. 2005).

[96] 2006 U.S. Dist. Lexis 4846 (D. Minn. 2006).

[97] 486 F.Supp.2d 705 (S.D. Ohio 2007).

[98] 499 F.3d 629 (7th Cir. 2007).

[99] The NIST Performance Measurement Guide for Information Security is available at http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

[100] *Id.*

[101] NIST publishes Federal Information Processing Standards that provide guidance for Federal Agencies. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems is available at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[102] ISO/IEC 27000 provides an overview of the ISO/IEC 27000-series and is available at http://webstore.iec.ch/preview/info_isoiec27000%7Bed1.0%7Den.pdf.

[103] Payment Card Industry, "Data Security Standard version 1.2", p. 3 (2008), http:// https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

[104] *Id.*, page 37 (Requirements 8.1, 8.2, 8.3 and 8.4).

[105] Several states have bans or restrictions on awarding contracts to service providers where the work will be performed outside of the U.S., including New Jersey, Missouri, and Michigan. Others require the service provider to disclose the intended place of performance.

[106] *See* Treasury Regulation § 301.7216-3, Rev. Proc. 2008-35.

[107] Nevertheless, the Federal Banking Agencies have issued guidance to banks regarding foreign-based service providers. *See* IT Examination Handbook-Outsourcing Technology Services, Appendix C.

[108] *See, e.g.*, Office of Thrift Supervision, Thrift Bulletin 82a (Mar. 2003); Federal Deposit Insurance Corporation, Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks (June 2004).

[109] 70 Fed. Reg. 15736 (2005).

[110] *See* FTC Press Release, "CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations," *supra* note 85.

[111] *See* FTC Press Release, "Consumer Electronics Company Agrees to Settle Data Security Charges; Breach Compromised Data of Hundreds of Consumers," *supra* note 83.

[112] *See* FTC Press Release, "Mortgage Company Settles Data Security Charges" (Nov. 6, 2008) (available at http://www.ftc.gov/opa/2008/11/pcl.shtm).

[113] *See* FTC Press Release, "Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data," *supra* note 80.

[114] *See id.*

[115] *See* FTC Press Release, "ValueClick to Pay $2.9 Million to Settle FTC Charges," *supra* note 83.

[116] *See* FTC Press Release, "Student Lender Settles FTC Charges" (Mar. 4, 2008) (available at http://www.ftc.gov/opa/2008/03/studlend.shtm).

[117] *See* FTC Press Release, "Online Apparel Life is Good Retailer Settles FTC Charges," *supra* note 80.

[118] Life is good, Inc., and Life is good Retail, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 73 Fed. Reg. 4231 (2008).

[119] *See* FTC Press Release, "Company Will Pay $50,000 Penalty for Tossing Consumers' Credit Report Information in Unsecured Dumpster" (Dec. 18, 2007) (available at http://www.ftc.gov/opa/2007/12/aumort.shtm).

[120] Guidance Software, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 71 Fed. Reg. 68628 (2006).

[121] *Id.*

[122] Guidance Software (decision and consent order), *supra* note 74, at 2.

[123] *Id.* at 3.

[124] *Id.*

[125] *See* FTC Press Release, "CardSystems Solutions Settles FTC Charges," *supra* note 80.

[126] *See* FTC Press Release, "DSW Inc. Settles FTC Charges," *supra* note 80.

[127] *Id.*

[128] *See* FTC Press Release, "ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress" (Jan. 26, 2006) (available at http://www.ftc.gov/opa/2006/01/choicepoint.shtm).

[129] *See* FTC Press Release, "BJ's Wholesale Club Settles FTC Charges," *supra* note 79.

[130] *Id.*

[131] 486 F.Supp.2d 705 (S.D. Ohio 2007).

[132] 499 F.3d 629 (7th Cir. 2007).
[133] D. Mass., No. 07-10162, MDL Docket No. 1838.