An Overview of Data Security Legal Requirements *for All Business Sectors*

Thomas J. Smedinghoff[1]

TABLE OF CONTENTS

Page

[1] Thomas J. Smedinghoff is a partner in the Privacy and Data Protection practice group at the law firm of Edwards Wildman Palmer LLP, in Chicago. Tom is a member of the ABA Cybersecurity Legal Task Force, and Chair of the Identity Management Legal Task Force and Co-Chair of the Cybersecurity Subcommittee of the ABA Section of Business Law, Cyberspace Committee. He is also a member of the U.S. Delegation to the United Nations Commission on International Trade Law ("UNCITRAL"), where he participated in the negotiation of the *United Nations Convention on the Use of Electronic Communications in International Contracts*. He is also the author of INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE (IT Governance Publishing, 2008). He can be reached at tsmedinghoff@edwardswildman.com.

TABLE OF CONTENTS
(continued)

Page

An Overview of
Data Security Legal Requirements
for All Business Sectors

What are the data security legal obligations generally applicable to all U.S. businesses?

It is well known that certain sectors of the U.S. economy are subject to extensive regulations regarding data security. The most obvious examples are the financial sector,[2] the healthcare sector,[3] the federal government sector,[4] and the target of current regulatory efforts, the critical infrastructure sectors.[5] But what about companies in non-regulated sectors?

There is also no doubt that non-regulated businesses are subject to data security obligations. One need look no further than the last 10 years of FTC and state attorney general enforcement actions to see that numerous non-regulated companies have been targeted for failure to provide appropriate data security for their own corporate data. Examples include software vendors (Microsoft[6] and Guidance Software[7]), consumer electronics companies (Genica and Computer Geeks),[8] mobile app developers (Delta Airlines),[9] clothing retailers (Guess![10] and Life Is Good[11]), music retailers (Tower Records),[12] animal supply retailers (PetCo),[13] general merchandise retail stores (BJs Wholesale,[14] TJX companies,[15] and Sears[16]), shoe stores

---

[2] Subject to the Gramm-Leach-Bliley Act ("GLB"), Public Law 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing regulations at 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314 (FTC) (emphasis added).

[3] Subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. 1320d-2 and 1320d-4, and HIPAA Security Regulations, 45 C.F.R. Part 164.

[4] Subject to the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Sections 3541-3549.

[5] See Presidential Executive Order, "Improving Critical Infrastructure Cybersecurity," February 12, 2013, at www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[6] FTC V. Microsoft (Consent Decree, Aug. 7, 2002), *available at* www.ftc.gov/os/caselist/0123240/0123240.shtm

[7] In the Matter of Guidance Software (Agreement Containing Consent Order, FTC File No. 062 3057, November 16, 2006), available at www.ftc.gov/opa/2006/11/guidance.htm

[8] In the Matter of Genica Corporation, and Compgeeks.com, FTC File No. 082-3113 (Agreement Containing Consent Order, February 5, 2009), available at www.ftc.gov/os/caselist/0823113

[9] See, "California Attorney General Sues Delta Air Lines for Failing to Have a Mobile App Privacy Policy," at http://bit.ly/W11J4T

[10] In the matter of Guess?, Inc. (Agreement containing Consent Order, FTC File No. 022 3260, June 18, 2003), *available at* www.ftc.gov/os/2003/06/guessagree.htm

[11] In the Matter of Life is good, Inc. (Agreement Containing Consent Order, FTC File No. 072 3046, January 17, 2008), available at www.ftc.gov/os/caselist/0723046

[12] In the Matter of MTS, Inc., d/b/a Tower records/Books/Video (Agreement containing Consent Order, FTC File No. 032-3209, Apr. 21, 2004), *available at* www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf

[13] In the Matter of Petco Animal Supplies, Inc. (Agreement containing Consent Order, FTC File No. 042 3153, Nov. 7, 2004), *available at* www.ftc.gov/os/caselist/0323221/0323221.htm

[14] In the Matter of BJ's Wholesale Club, Inc. (Agreement containing Consent Order, FTC File No. 042 3160, June 16, 2005), *available at* www.ftc.gov/opa/2005/06/bjswholesale.htm

[15] In The Matter of The TJX Companies, Inc., FTC File No. 072-3055 (Agreement Containing Consent Order, March 27, 2008), available at www.ftc.gov/os/caselist/0723055

[16] In the Matter of Sears Holdings Management Corporation, FTC File No. 082 3099 (Agreement Containing Consent Order, September 9, 2009), available at http://www.ftc.gov/os/caselist/0823099/index.shtm

(DSW),[17] restaurant and entertainment establishments (Dave & Busters[18] and Briar Group[19]), social media sites (Twitter[20] and Facebook[21]), bookstores (Barnes & Noble),[22] property management firms (Maloney Properties, Inc.),[23] and hotels (Wyndham).[24]

The thesis of this paper is that all businesses, whether regulated or not, are generally subject to legal duties regarding the security of their corporate data. Those duties can be summarized as: (1) a duty to protect the security of their corporate data, and (2) a duty to disclose security breaches when they occur. The following sections will explain the source and scope of those duties. But first we begin with a general overview of the concept of data security itself.

A. WHAT IS DATA SECURITY?

Security is the protection of assets (such as buildings, equipment, cargo, inventory, and in some cases, people) from threats. Data security (or information security) has been generally described as "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities,"[25] and as "the process by which an organization protects and secures systems, media, and facilities that process and maintain information vital to its operations."[26]

The terms data security, information security and cybersecurity are often used interchangeably, although some might argue that each has a somewhat different emphasis. But regardless of the label, the focus is on the protection of both (1) *information systems*[27] -- i.e., computer systems, networks, and software, and (2) the *data, messages, and information* that are typically recorded on, processed by, communicated via, stored in, shared by, transmitted, or received from such information systems.[28]

---

[17] In the Matter of DSW Inc., (Agreement containing Consent Order, FTC File No. 052 3096, Dec. 1, 2005), *available at* www.ftc.gov/opa/2005/12/dsw.htm

[18] In the Matter of Dave & Buster's, Inc., FTC File No. 082 3153 (Agreement Containing Consent Order, March 25, 2010), available at http://www.ftc.gov/os/caselist/0823153/index.shtm

[19] See "Massachusetts Attorney General Breaking New Ground in Data Security Enforcement?" at http://bit.ly/15rGiz4.

[20] In the Matter of Twitter, Inc., FTC File No. 092 3093 (Agreement Containing Consent Order, June 24, 2010; Decision and Order, March 11, 2011), available at http://www.ftc.gov/os/caselist/0923093a/index.shtm

[21] In the Matter of Facebook, Inc., File No 092 3184 (Agreement Containing Consent Order, November 29, 2011), available at http://ftc.gov/os/caselist/0923184/index.shtm

[22] http://www.steptoe.com/assets/attachments/514.pdf

[23] See, "Massachusetts Attorney General Announces $15,000 Settlement with Property Management Firm" at http://bit.ly/GU8iNU.

[24] FTC v. Wyndham Worldwide Corp., 2014 U.S. Dist. LEXIS 47622 (D. N.J., April 7, 2014). Complaint and other information at http://www.ftc.gov/opa/2012/06/wyndham.shtm).

[25] ISO/IEC 27002:2005, *Information Technology – Security Techniques – Code of Practice for Information Security Management* (June. 2005), at p. viii (hereinafter "ISO 27002").

[26] FFIEC, *IT Examinations Handbook – Information Security* (July 2006) at p. 1; available at http://ithandbook.ffiec.gov/it-booklets.aspx.

[27] The Homeland Security Act of 2002 defines the term "information system" to mean "any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes – (A) computers and computer networks; (B) ancillary equipment; (C) software, firmware, and related procedures; (D) services, including support services; and (E) related resources." Homeland Security Act of 2002, Pub. L. 107-296, at Section 1001(b), amending 44 U.S.C. § 3532(b)(4).

[28] The *data, messages, and information* to be protected potentially includes a wide variety of data, such as personally identifiable information about employees, customers, prospects, and other individuals; corporate financial information, information regarding

Measures designed to protect the security of information systems and data are generally grouped into three categories, which are typically referred to as follows:

- **Physical security measures:** These are security measures which are designed to protect the tangible items that comprise the physical computer systems and networks that process, communicates, and store the data, including servers, devices used to access the system, storage devices, and the like. Examples include fences, walls, and other barriers; locks, safes, and vaults; armed guards; sensors and alarm bells.
- **Technical security measures:** These are security measures which involve the use of safeguards incorporated into computer hardware, software, and related devices. They are designed to ensure system availability, control access to systems and information, authenticate persons seeking access, protect the integrity of information communicated via and stored on the system, and ensure confidentiality where appropriate. Examples include: firewalls, intrusion detection software, access control software, antivirus software, passwords, PIN numbers, smart cards, biometric tokens, and encryption processes.
- **Administrative security measures:** Sometimes referred to as "procedural" or "organizational" security measures, these are security measures which consist of management procedures and constraints, operational procedures, accountability procedures, policies, and supplemental administrative controls to prevent unauthorized access and to provide an acceptable level of protection for computing resources and data. Administrative security procedures frequently include personnel management, employee use policies, training, and discipline.

Within each of these three categories, security measures are further classified as preventative, detective, or reactive. *Preventative* security measures are designed to prevent the occurrence of events that compromise security. An example of a preventative security measure is a lock on a door (to prevent access to a room containing computer equipment), or a firewall (to prevent unauthorized online access to a computer system). *Detective* security measures are designed to identify security breaches after they have occurred. An example of a detective security measure is a smoke alarm (which is designed to detect a fire), or intrusion detection software (which is designed to detect and track unauthorized online access to a computer system). *Reactive* security measures are designed to respond to a security breach, and typically include efforts to stop or contain the breach, identify the party or parties involved, and allow recovery of information that is lost or damaged. An example of reactive security is calling the police after an alarm detects that a burglary is in process, or shutting down a computer system after intrusion detection software determines that an unauthorized user has obtained access to the system.

The objectives to be achieved through the use of security measures can be defined in terms of either the positive results to be achieved or the negative consequences to be avoided. The positive results to be achieved are typically described as (1) ensuring the *availability* of systems and information, (2) controlling *access* to systems and information, and (3) ensuring the *confidentiality, integrity, authenticity* of information[29] The harms to be avoided are often described as unauthorized access, use, disclosure or transfer, modification, alteration, or processing of data, and accidental loss or destruction of data.[30]

---

corporate business transactions, trade secrets and other confidential information, information relating to corporate communications, including e-mail, and a variety of other types of corporate data. It can also take a variety of forms, including data, messages, documents, voice recordings, images, video, software, and other content in both electronic and paper form.

[29] *See, e.g.*, Homeland Security Act of 2002 (Federal Information Security Management Act of 2002) 44 U.S.C. Section 3542(b)(1); GLB Security Regulations (OCC), 12 C.F.R. Part 30 Appendix B, Part II.B; HIPAA Security Regulations, 45 C.F.R. Section 164.306(a)(1); Microsoft Consent Decree at II, p. 4.

[30] *See, e.g.*, 44 USC 3532(b)(1), emphasis added. See also FISMA, 44 U.S.C. Section 3542(b)(1). Most of the foreign privacy laws also focus their security requirements from this perspective. This includes, for example, the EU Data Protection Directive,

Achieving these objectives involves implementing security measures designed to protect systems and information from the various threats they face. What those threats are, where they come from, what is at risk, and how serious the consequences are, will of course, vary greatly from case to case. But responding to the threats a company faces with appropriate physical, technical, and organizational security measures is the focus of the duty to provide security.

B. THE DUTY TO PROVIDE SECURITY

Concerns regarding individual privacy, corporate governance, accountability for financial information, the authenticity and integrity of transaction data, and the security of sensitive business data are driving the enactment of new laws and regulations designed to ensure that businesses adequately address the security of their own data. In addition to sector-specific regulations, legislative and regulatory initiatives are imposing obligations on all businesses to implement information security measures to protect their own data and to disclose breaches of security that do occur.

1. Where Does the Duty to Provide Security Come From?

There is no single law, statute, or regulation that governs a non-regulated company's obligations to provide security for its information. Corporate legal obligations to implement security measures are set forth in an ever-expanding patchwork of generally-applicable state, federal, and international laws, regulations, and enforcement actions, as well as common law duties and other express and implied obligations to provide "reasonable" or "appropriate" security for corporate data. And these obligations apply to both regulated and non-regulated industries.

When viewed as a group they cover a large segment of corporate activity. The most common sources of obligations of non-regulated companies to provide data security include the following:

(a) Statutes and Regulations

Numerous statutes and regulations impose obligations on businesses to provide security. Some are sector-specific comprehensive security regulations. Other generally-applicable laws are readily recognized by the fact that they are labeled as security laws or use terms such as "security," "safeguards," or "protection."[31] But in many cases the fact that they impose security obligations is evident only by their inclusion or use of terms relating to the attributes of security, such as "authenticate," "integrity," "confidentiality," "availability of data," and the like.[32] Some of the most common sources of statutory and regulatory obligations to provide cybersecurity include:

Article 17(1); Albania Act, Article 9; Argentina Act, Article 9(1); Australia Act, Schedule 3, Section 4.1; Austria Act, Section 14(1); Belgium Act, Art. 16(4); Canada Act, Schedule 1, Section 4.7.1; Denmark Act, Section 41(3); Estonia Act, Section 19(1) and (2); Finland Act, Section 32(1); France Act, Article 34; German Act, Annex (to the first sentence of Section 9), Sections 1, 2, and 4; Greece Act, Article 10(3); Hong Kong Act, Principle 4; Hungary Act, Article 10(2); Ireland Act, Section 2-(1)(d), and First Schedule, Article 7; Italy Act, Section 31; Lithuania Act, Article 24(1); Netherlands Act, Article 13; Philippines Act, Article 8.1; Poland Act, Articles 7 and 36; Portugal Act, Article 14(1); Russia Act, Section 19(1); Singapore Model Code, Principle 7, Section 4.7.1; Slovakia Act, Section 15(1); Spain Act, Article 9; United Arab Emirates Act, Articles 15(1) and 16(1); UK Act, Schedule 1, Part I, Seventh Principle.

[31] See, e.g., Standards for the Protection of Personal Information of Residents of the Commonwealth, Massachusetts 201 CMR 17; and Business Duty to Protect Sensitive Personal Information, Tex. Bus. & Com. Code § 521.052.

[32] *See, e.g.*, E-SIGN, 15 USC 7001 et seq. and UETA.

Privacy Laws. The obligation to provide adequate security for personal data collected, used, and/or maintained by a business is a critical component of almost all privacy laws. Most statements of basic privacy principles include security as a key component,[33] and most privacy laws and regulations typically require companies to implement information security measures to protect certain personal data they maintain about individuals.

In the United States protecting personal information is the focus of numerous federal and state privacy laws and regulations. In addition to sector-specific privacy laws and regulations such as GLB (financial sector), HIPAA (healthcare sector), and the Privacy Act of 1974 (federal government), the US-EU Safe Harbor Framework[34] and numerous federal and state privacy laws that target specific types of data also include security requirements. This includes the federal Children's Online Privacy Protection Act (COPPA), which applies to all businesses collecting personal information on the Internet from children, as well as numerous state laws relating to credit card information, personal information, and social security numbers.[35]

Data Security Laws. Separate from privacy laws, several states have enacted laws imposing a general obligation on all companies to ensure the security of personal information. The first was California, which enacted legislation in 2004 requiring all businesses to "implement and maintain reasonable security procedures and practices" to protect personal information about California residents from unauthorized access, destruction, use, modification, or disclosure.[36] Several other states have followed suit. State laws governing secure data destruction also fall in to this category.

Some federal regulations also impose a duty to provide for the security of data and systems. Examples include IRS regulations that require companies to implement information security to protect electronic tax records, and SEC regulations regarding protection of corporate financial data.[37]

E-Transaction Laws. E-transaction laws require appropriate data security to ensure the enforceability of electronic records and for compliance with electronic recordkeeping requirements. Both the federal and state electronic transaction statutes (E-SIGN and UETA) require all companies to provide security for storage of electronic records relating to online transactions. For example, they focus on the security requirements of data integrity and accessibility, and require that an electronic record must "accurately reflect the information set forth in the record after it was first generated in its final form," and that it must "remain accessible for later reference."[38]

---

[33] *See, e.g.*, Consumer Privacy Bill of Rights in White House Report "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012; available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; Australia, Information Privacy Principles under the Privacy Act 1988, Principle No. 4, available at www.privacy.gov.au/publications/ipps.html; AICPA and the Canadian Institute of Chartered Accountants (CICA), Generally Accepted Privacy principles, Principle No. 8, available at http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles; APEC, Privacy principles, Principle No. 7, available at http://austlii.edu.au/~graham/APEC/APECv10.doc; US-EU Safe Harbor Privacy Principles, available at www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm; Direct Marketing Association, Online Marketing Guidelines, available at www.the-dma.org/guidelines/onlineguidelines.shtml.

[34] http://export.gov/safeharbor

[35] These include Arkansas, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah.

[36] Cal. Civ. Code § 1798.81.5(b).

[37] See, e.g., IRS Regulations: Rev. Proc. 97-22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25, and SEC Regulations: 17 C.F.R. 240.17a-4, 17 C.F.R. 257.1(e)(3), and 17 C.F.R. § 248.30

[38] See e.g., UETA at Section 12. See also E-SIGN at 15 USC Sections 7001(d) and (e).

Corporate Governance Legislation. Corporate governance legislation designed to protect the company and its shareholders, investors, and business partners, such as Sarbanes-Oxley and implementing regulations, require public companies to ensure that they have implemented appropriate information security controls with respect to their financial information.[39] In addition, SEC disclosure guidance issued on October 13, 2011[40] identifies cyber risks and incidents as potential material information to be disclosed under existing securities law disclosure requirements and accounting standards.

Unfair & Deceptive Business Practice Laws. Unfair business practice laws (such as FTC Act Section 5,[41] which prohibits "unfair or deceptive acts or practices in or affecting commerce," and equivalent state laws) and related government enforcement actions are frequently used as a basis for regulating security.

Through a series of enforcement actions and consent decrees beginning in 2002,[42] both the FTC and several state attorneys general have, in effect, extended security obligations regarding personal information to non-regulated industries by virtue of Section 5 of the FTC Act and similar state laws. Initially, cases were based on the alleged failure of companies to provide adequate information security contrary to representations they made to customers. In other words, these were claims of deceptive trade practices. But beginning in June 2005, the FTC significantly broadened the scope of its enforcement actions by asserting that a failure to provide appropriate information security for consumer personal information was itself, an unfair trade practice – even in the absence of any false representations by the defendant as to the state of its security.[43]

Breach Notification Laws. In addition to the legal obligation to *implement* security measures to protect corporate data, many laws impose an obligation to *disclose* security breaches to the persons affected. But unlike laws that impose a duty to provide security, these laws typically require only that companies disclose security breaches to those who may be adversely affected by such breaches.[44]

A total of 46 states in the U.S., plus the District of Columbia, Puerto Rico, and the Virgin Islands, have enacted security breach notification laws, all generally based on a 2003 California law.[45] The U.S. federal banking regulatory agencies also require financial institutions to disclose breaches,[46] and the HITECH Act and associated regulations also require notice in the event of a breach.[47]

---

[39] See generally, Bruce H. Nearon, Jon Stanley, Steven W. Teppler, and Joseph Burton, Life after Sarbanes-Oxley: The Merger of Information Security and Accountability, 45 Jurimetrics Journal 379-412 (2005).

[40] SEC Guidance: SEC CF Disclosure Guidance: Topic No. 2, Cybersecurity; http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[41] 15 USC Section 45.

[42] See e.g., FTC enforcement actions cited at footnotes 9 to 27 above.

[43] The FTC's authority to proceed in this manner was recently upheld in FTC v. Wyndham Worldwide Corp., 2014 U.S. Dist. LEXIS 47622 (D. N.J., April 7, 2014).

[44] *Pisciotta v. Old National Bancorp*., 2007 U.S. App. Lexis 20068 (7th Cir. 23 August 2007), at p. 13.

[45] See list at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. The only states without breach notification laws are Alabama, Kentucky, New Mexico, and South Dakota.

[46] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (OCC), 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), March 29, 2005, Federal Register, Vol. 70, No. 59, 29 March 2005, at p. 15736 (hereinafter "Interagency Guidance").

[47] 45 CFR Part 164.

(b) Common Law Obligations

Some case law also recognizes that there may be a common law duty to provide data security, the breach of which constitutes a tort. In *Bell v. Michigan Council*, for example, the court held that "defendant did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information."[48] Likewise, in the case of *In re: Sony Gaming Networks and Customer Data Security Breach Litigation*, the court recognized the existence of a legal duty to provide security, noting as follows:

> Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law. See, e.g., *Witriol v. LexisNexis Grp.*, No. C05-02392 MJJ, 2006 WL 4725713, at *8 (N.D. Cal. Feb. 10, 2006); *CUMIS Ins. Soc'y., Inc. v. BJ's Wholesale Club, Inc.*, No. 051158, 2005 WL 6075375, at *4 (Mass. Super. Dec. 7, 2005) aff'd, 918 N.E.2d 36 (Mass. 2009); *Yakubowicz v. Paramount Pictures Corp.*, 536 N.E.2d 1067, 1070 (Mass. 1989) ("A basic principle of negligence law is that ordinarily everyone has a duty to refrain from affirmative acts that unreasonably expose others to a risk of harm."). As a result, because Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach.[49]

In at least one case, however, a court held that there is no common law duty to provide security.[50]

(c) Rules of Evidence

Providing appropriate security necessary to ensure the integrity of electronic records (and, where necessary, the identity of the creator, sender, or signer of the record) will likely be critical to the admissibility of the electronic record in evidence in a future dispute. This conclusion is supported both by recent case law[51] as well as provisions relating to the form requirement for an "original" in electronic transaction legislation.[52]

In particular, the Ninth Circuit decision in the case of *American Express v. Vinhnee*[53] suggests that use of appropriate security may be a condition for the admissibility in evidence of electronic records. The bottom line is that, in many situations, the admissibility of all types of electronic data will depend, on the level of information security provided in order to ensure that the integrity and availability of the information remains intact.

---

[48] *Bell v. Michigan Council*, 205 Mich. App. Lexis 353 at *16 (Mich. App. 2005).

[49] *In re: Sony Gaming Networks and Customer Data Security Breach Litigation*, 2014 BL 15530, (S.D. Cal., No. 3:11-md-02258-AJB-MDD, partially dismissed Jan 21, 2014), at pp. 21-22.

[50] *Cooney v. Chicago Public Schools*, 2010 Ill. App. LEXIS 1424 (December 30, 2010).

[51] *See, e.g., American Express v. Vinhnee*, 2005 Bankr. Lexis 2602 (9th Cir. Bk. App. Panel, 2005); *Lorraine v. Markel*, 2007 U.S. Dist. Lexis 33020 (D. MD. May 4, 2007).

[52] See, e.g., UETA Section 12, and E-SIGN, 15 USC Section 7001(d).

[53] *American Express v. Vinhnee*, 336 B.R. 437; 2005 Bankr. Lexis 2602 (9th Cir. December 16, 2006).

(d) Contractual Obligations

Data security obligations are often imposed by contract as well. As businesses increasingly become aware of the need to protect the security of their own data, they frequently try to satisfy their obligation (at least in part) by contract in those situations where third parties will have possession of, or access to, their business data. This is particularly common, for example, in outsourcing and cloud service arrangements where a company's data will be stored with and/or processed by a third party. In addition, in any situation where a business may have access to data of a trading partner, it is quite common for the trading partner to contractually impose security obligations with respect to that data.

Security obligations are also typically imposed by contract in connection with participation in a multi-party system. For example, merchants desiring to accept credit cards must contractually agree to comply with the requirements of the Payment Card Industry Data Security Standard[54] as a condition of accepting credit cards. Similarly, businesses that want to originate electronic payment orders (e.g., to debit a customer's bank account) must agree to the rules of the applicable electronic payment systems (such as the ACH payment system), which rules include data security provisions.

(e) Self-Imposed Obligations

In many cases, security obligations are also self-imposed. This commonly occurs, for example, through statements in privacy policies, on websites, or in advertising materials, companies often make representations regarding the level of security they provide for their data (particularly the personal data they collect from the persons to whom the statements are made). Likewise, when companies voluntarily self-certify under the U.S.-EU Safe Harbor Framework,[55] they represent that they comply with the seven Safe Harbor Privacy Principles. Those Principles include a security requirement that "in creating, maintaining, using or disseminating personal information," the certifying organization "must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction."[56]

By making such public statements or representations, companies impose on themselves an obligation to comply with the standard they have represented to the public that they meet. If those statements are not true, or if they are misleading, such statements may become, in effect, deceptive trade practices under Section 5 of the FTC Act, or under equivalent state laws. Through a series of enforcement actions and consent decrees, both the FTC and several state attorneys general have used those deceptive business practice statutes to bring enforcement actions against the offending companies.

2. What Is the Nature of the Legal Obligation?

The duty to provide data security is often simply stated in the law as an obligation to implement "reasonable" or "appropriate" security measures designed to achieve the security objectives noted above.

In Europe, for example, individual country implementations of the EU Data Protection Directive generally require the use of security measures that are *appropriate* to protect the personal data[57] or that are *necessary* to protect the personal data.[58]

---

[54] Available at www.pcisecuritystandards.org.

[55] See generally http://export.gov/safeharbor.

[56] See Safe Harbor Privacy Principles at http://export.gov/safeharbor/eu/eg_main_018475.asp.

[57] *See, e.g.*, Belgium – Belgian Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, as modified by the law of 11 December 1998 Implementing Directive 95/46/EC, and the law of 26 February 2003, Chapter IV,

In the United States, state security laws, such as in California, generally require "reasonable security procedures and practices."[59] Even HIPAA requires "*reasonable and appropriate" security*,[60] and the GLB security regulations require security *appropriate* to the size and complexity of the bank and the nature and scope of its activities."[61]

In other words, the law views security is a relative concept, and recognizes that what qualifies as reasonable security varies with the situation. Thus, the law typically provides little or no guidance on what specific security measures are required, or on how much security a business should implement to satisfy those legal obligations. Most laws do not include any specific requirements regarding whether or not a particular security measure must be implemented,[62] and there are generally no safe harbors. In light of such standards, the choice of security measures and technology can vary depending on the situation.

3. What Is the Legal Standard for Compliance? Defining "Reasonable" Security

Laws requiring that companies implement "reasonable" or "appropriate" security often provide little or no guidance as to what is required for legal compliance. Legal developments over the past few years, however, suggest that a legal standard for "reasonable" security is clearly emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like), and instead adopts a fact-specific approach to corporate security obligations that requires a "process" applied to the unique facts of each case. It puts the focus on identifying and responding to the particular threats a business faces.

Rather than telling companies what specific security measures they must implement, the emerging legal standard requires companies to engage in an ongoing and repetitive process that is designed to identify and assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments. The decision regarding the specific security measures is left up to the company.

Article 16(4); Denmark – Act on Processing of Personal Data,; *Act No. 429 of 31 May 2000,* (unofficial English translation), Title IV, Part 11, Section 41(3); Estonia -- Personal Data Protection Act; Passed 12 February 2003 (RT[1] I 2003, 26, 158), entered into force 1 October 2003, Chapter 3, Sections 19(2); Greece – Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended by Laws 2819/2000 and 2915/2001); Article 10(3); Ireland –Data Protection (Amendment) Act 2003; Section 2.-(1)(d) and First Schedule Article 7; Lithuania – Law on Legal Protection of Personal Data, 21 January 2003, No. IX-1296, Official translation, with amendments 13 April 2004, Article 24(1); Netherlands – 25 892 - Rules for the protection of personal data (Personal Data Protection Act) (Unofficial translation); Article 13; Portugal – Act on the Protection of Personal Data (transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), Article 14(1); Slovakia – Act No 428 of 3 July 2002 on personal data protection; Section 15(1); Sweden – Personal Data Act (1998:204); issued 29 April 1998, Section 31; and UK – Data Protection Act 1998, Schedule 1, Part I, Seventh Principle

[58] *See, e.g.,* Finland – The Finnish Personal Data Act (523/1999), given on 22.4.1999, Section 32(1); Germany – Federal Data Protection Act as of 1 January 2003, Section 9; Hungary – Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest, Article 10(1); Italy – Personal Data Protection Code, Legislative Decree No. 196 of 30 June 2003, Sections 31 and 33; Spain – Organic Law 15/1999 of 13 December on the Protection of Personal Data, Article 9

[59] Cal. Civil Code § 1798.81.5(b).

[60] 42 U.S.C. 1320d-2(d)(2).

[61] See, Gramm-Leach-Bliley Act ("GLB"), Public Law 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing regulations at 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314 (FTC) (emphasis added).

[62] There are some exceptions, however. For example, the Massachusetts security regulations require implementation of firewalls, the use of virus software, and in certain cases, the use of encryption. See 201 CMR 17.

This approach recognizes that there are a variety of different security measures responsive to specific threats, and recognizes that threats (and appropriate responsive security measures) are constantly changing. Thus, the presence or absence of specific security measures says little about the status of a company's legal compliance with its information security obligations. Because armed guards at a the front of a building do not protect against hackers accessing information through the Internet, and because firewalls designed to stop hackers do not protect against dishonest employees with authorized access, the law puts its focus on implementing those security measures that respond to the specific threats a business faces.

At its essence implementing "reasonable" or "appropriate" security compliance requires a company to implement a process-oriented approach whereby it does the following:

- **Assign Responsibility:** Designate one or more employees to maintain the security program;
- **Identify Information Assets**: Identify the corporate information assets that need to be protected, including records containing personal information and computing systems and storage media (such as laptops and portable devices) used to store such personal information;
- **Conduct Risk Assessment:** Conduct a risk assessment to identify and assess internal and external risks to the security, confidentiality, and/or integrity of its information assets, and evaluate the effectiveness of the safeguards currently in place for minimizing such risks;
- **Select and Implement Responsive Security Controls:** Select and implement appropriate physical, administrative, and technical security controls to minimize the risks identified in its risk assessment, including security controls within certain identified "categories" (discussed below);
- **Monitor Effectiveness:** Regularly monitor and test the security controls it has implemented to ensure that the security program is operating in a manner reasonably calculated to protect the personal information; and upgrade the security controls as necessary to limit risks;
- **Regularly Review Program:** Review and adjust the information security program at least annually, including: (i) whenever there is a material change in business practices that could affect personal information, and (ii) following any incident involving a breach of security; and
- **Address Third Party Issues:** Take all reasonable steps to verify that each third-party service provider that has access to personal information has the capacity to protect such information in the manner provided for in the Massachusetts Regulations; and take all reasonable steps to ensure that each third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied under the Massachusetts Regulations (discussed below).

A key aspect of this process is recognition that it is never completed. It is ongoing, and must be continually reviewed, revised, and updated.

This "process oriented" legal standard for corporate information security has come to be known as a requirement to develop, implement, maintain and regularly monitor and update a comprehensive information security program (WISP).[63]

[63] *See, e.g.*, Massachusetts Security Regulations, 201 CMR 17.03. *See also* Massachusetts Office of Consumer Affairs, "Small Business Guide: Formulating A Comprehensive Written Information Security Program," available at http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf. See also, Information Security and Security Breach Notification Guidance, published by the Illinois Attorney General's Office, at http://illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guideance.pdf.

The requirement for a such a security program was first set forth in a series of financial industry security regulations required under the Gramm-Leach-Bliley Act (GLBA) titled *Guidelines Establishing Standards for Safeguarding Consumer Information.* They were issued by the Federal Reserve, the OCC, FDIC, and the Office of Thrift Supervision, on February 1, 2001,[64] and later adopted by the FTC in its GLBA *Safeguards Rule* on May 23, 2002.[65] The same approach was also incorporated in the Federal Information Security Management Act of 2002 ("FISMA"),[66] and in the HIPAA *Security Standards* issued by the Department of Health and Human Services on February 20, 2003.[67]

The FTC has since adopted the view that the process oriented approach to information security outlined in these regulations sets forth a general "best practice" for legal compliance that should apply to all businesses in all industries.[68] Thus, the FTC has, in effect, implemented this process oriented requirement for compliance in all of its decisions and consent decrees relating to alleged failures to provide appropriate information security.[69] The National Association of Insurance Commissioners has also recommended the same approach, and to date, several state insurance regulators have adopted it.[70]

In 2010 this approach was formally adopted by Massachusetts in its data security regulations, which require businesses to develop a comprehensive written information security program, and set out detailed requirements for such a security program.[71]

In the EU, a similar requirement is specifically referenced in some country statutes.[72] In addition, several country statutes incorporate the various elements of the process, including conducting periodic risk assessments,[73] developing and implementing a responsive security program[74] including employee

---

[64] 66 Fed. Reg. 8616, February 1, 2001; 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision).

[65] 67 Fed. Reg. 36484, May 23, 2002; 16 C.F.R. Part 314.

[66] 44 U.S.C. Section 3544(b).

[67] 45 C.F.R. Parts 164.

[68] See, Prepared Statement of the Federal Trade Commission on Identity Theft: Innovative Solutions For An Evolving Problem, Presented by Lydia Parnes, Director, Bureau of Consumer Protection, Before the Subcommittee On Terrorism, Technology and Homeland Security of the Senate Committee on the Judiciary, United States Senate**,** March 21, 2007 at p. 7 (noting that "the FTC Safeguards Rule promulgated under the GLB Act serves as a good model" for satisfying the obligation to maintain reasonable and appropriate security); available at www.ftc.gov/os/testimony/P065409identitytheftsenate03212007.pdf. See also, Prepared Statement of the Federal Trade Commission before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, U.S. House of Representatives on "Protecting Our Nation's Cyberspace," April 21, 2004, at p. 5 (noting that "security is an ongoing process of using reasonable and appropriate measures in light of the circumstances"), available at www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf.

[69] *See, e.g.*, FTC Decisions and Consent Decrees listed in the Appendix.

[70] *See, e.g.*, National Association of Insurance Commissioners "Standards for Safeguarding Customer Information Model Regulation" IV-673-1 available at www.naic.org.

[71] 201 CMR 17.00 et. seq.

[71] 201 CMR 17.00 et. seq.

[72] *See, e.g.*, Italy – Personal Data Protection Code, Legislative Decree No. 196 of 30 June 2003, Annex B, § 19.3; Slovakia Act No 428 of 3 July 2002 on personal data protection, § 16(5).

[73] From Appendix, see Italy Act, Annex B, Section 19.3; Slovak Republic Act, Section 16(5)

[74] From Appendix, see Argentina Act, Article 9(1); Estonia Act, Section 19(1); Belgium Act, Art. 16(4); Denmark Act, Section 41(3); Estonia Act, Section 19(1) ("IT"); Finland Act, Section 32(1); German Act, Section 9; Greece Act, Article 10(3); Hungary Act, Article 10(1); Lithuania Act, Article 24(1); Netherlands Act, Article 13; Portugal Act, Article 14(1); Slovak Republic Act, Section 15(1); Spain Act, Article 9; Sweden Act, Section 31; UK Act, Schedule 1, Part I, Seventh Principle; Swiss Act, Article 7.

training and education,[75] monitoring and testing the program,[76] continually reviewing and adjusting the program,[77] and overseeing third party service provider arrangements.[78]

In sum, the legal approach recognizes what security consultants have been saying for some time: "security is a process, not a product."[79] Legal compliance with security obligations involves a process applied to the facts of each case in order to achieve an objective (i.e., to identify and implement the security measures appropriate for that situation), rather than the implementation of standard specific security measures in all cases. Thus, there will likely be no hard and fast rules. Instead, the legal obligation regarding security focuses on what is reasonable under the circumstances to achieve the desired security objectives.

The requirement to develop a comprehensive information security program as the means of achieving reasonable security may be summarized as follows:

(a) Identify Information Assets

When addressing information security, the first step is to define the scope of the effort. What information, communications, and processes are to be protected? What information systems are involved? Where are they located. What laws potentially apply to them? As is often the case, little known but sensitive data files are found in a variety of places within the company.

(b) Conduct a Periodic Risk Assessment

Implementing a comprehensive security program to protect these assets requires a thorough assessment of the potential risks to the organization's information systems and data.

A risk assessment focuses on identifying foreseeable threats to corporate information and information systems. And it clearly plays a key role in determining whether a duty will be imposed and liability found. In *Wolfe v. MBNA America Bank*, for example, a federal court held that where injury resulting from negligent issuance of a credit card (to someone who applied using the plaintiff's identity) is foreseeable and preventable, "the defendant has a duty to verify the authenticity and accuracy of a credit account application."[80] In *Bell v. Michigan Council*, the court held that where a harm was foreseeable, and the potential severity of the risk was high, the defendant was liable for failure to provide appropriate security to address the potential harm.[81] On the other hand, in *Guin v. Brazos Education*, the court held

[75] From Appendix, see Australia Act, Schedule 2, Section 3.1(b); Belgium Act, Art 16(2)(3); Canada Act, Schedule 1, 4.7 Principle 7, Clause 4.7.4; Estonia Act, Section 20(3); Ireland Act, Section 2C(2); Italy Act, Annex B, Sections 4 and 19.6; Slovak Republic Act, Sections 17 and 19(3).

[76] From Appendix, see German Act, Section 9a (audit); Poland Ordinance, Attachment A (Basic Security Measures) § VII (monitor); Slovak Republic Act, Section 16(6)(d); Spain Royal Decree 994/1999 – Medium (audit).

[77] From Appendix, see Spain Royal Decree 994/1999 – Basic.

[78] From Appendix, see Australia Act, Section 14, Principle 4; Austria Act, Article 15(2); Belgium Act, Article 16; Denmark Act, Sections 41 and 42; Estonia Act, Section 20; Finland Act, Section 32(2); Ireland Act, Section 2C-(3); Italy Act, Annex B, Sections 4 and 19.6; Slovak Republic Act, Sections 17 and 19(3).

[79] Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (John Wiley & Sons, 2000) at page XII.

[80] Wolfe v. MBNA America Bank, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007).

[81] *See* Bell v. Michigan Council, 2005 Mich. App. Lexis 353 (Mich. App. February 15, 2005).

that where a proper risk assessment was done, but a particular harm was not reasonably foreseeable, the defendant would not be liable for failure to defend against it.[82]

Conducting a risk assessment begins with identifying all reasonably foreseeable internal and external threats to the information assets to be protected. Threats should be considered in each area of relevant operation, including information systems, network and software design, information processing, storage and disposal, prevention, detection, and response to attacks, intrusions, and other system failures, as well as employee training and management.

For each identified threat, the organization should then evaluate the risk posed by the threat by:

- Assessing the likelihood that the threat will materialize;
- Evaluating the potential damage that will result if it materializes; and
- Assessing the sufficiency of the policies, procedures, and safeguards in place to guard against the threat.

Such risk should be evaluated in light of the nature of the organization, its transactional capabilities, the sensitivity and value of the stored information to the organization and its trading partners, and the size and volume of its transactions.

This process will be the baseline against which security measures can be selected, implemented, measured, and validated. The goal is to understand the risks the business faces, and determine what level of risk is acceptable, in order to identify appropriate and cost-effective safeguards to combat that risk.

For general information on conducting a risk assessment, see The National Institute of Standards and Technology (NIST) special publication 800-30 "Guide for Conducting Risk Assessments."[83] Massachusetts also provides guidance in its "Small Business Guide: Formulating A Comprehensive Written Information Security Program."[84]

(c) Select and Implement Responsive Security Controls to Manage and Control Risk

Key to providing reasonable security is implementing security measures that are responsive to the specific risks that a company faces. In other words, merely implementing seemingly strong security measures is not, by itself, sufficient for legal compliance. Those security measures must be responsive to the particular threats a business faces, and must address its vulnerabilities. Posting armed guards around a building, for example, sounds impressive as a security measure, but if the primary threat the company faces is unauthorized remote access to its data via the Internet, that particular security measure is of little value. Likewise, firewalls and intrusion detection software are often effective ways to stop hackers, but if a company's major vulnerability is careless (or malicious) employees who inadvertently (or intentionally) disclose passwords, then even those sophisticated security measures, although important, will not adequately address the latter problem.

---

[82] *See* Guin v. Brazos Higher Education Service, Civ. No. 05-668, 2006 U.S. Dist. Lexis 4846 at *13 (D. Minn. Feb. 7, 2006) (finding that where a proper risk assessment was done, the inability to foresee and deter a specific burglary of a laptop was not a breach of a duty of reasonable care).

[83] *See* National Institute of Standards and Technology, "Risk Management Guide for Information Technology Systems," NIST Special Publication No. 800-30; available at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[84] *See* Massachusetts Office of Consumer Affairs, "Small Business Guide: Formulating A Comprehensive Written Information Security Program," available at http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf. See also, Information Security and Security Breach Notification Guidance, published by the Illinois Attorney General's Office, at http://illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guideance.pdf.

Thus, based on the results of the risk assessment, businesses must design and implement a security program consisting of reasonable physical, technical, and administrative security measures to manage and control the risks identified during the risk assessment. The security program should be in writing, and should be designed to provide reasonable safeguards to control the identified risks (i.e., to protect against any anticipated threats or hazards to the security or integrity of the information and systems to be protected). The goal is to reduce the risks and vulnerabilities to a reasonable and appropriate level.[85]

(1) Relevant Factors to Consider

In determining what security measures should be implemented within a particular organization, existing precedent recognizes that there is no "one size fits all" approach. Which security measures are appropriate for a particular organization will vary, depending upon a variety of factors.

Traditional negligence law suggests that the relevant factors are (1) the probability of the identified harm occurring (i.e., the likelihood that a foreseeable threat will materialize), (2) the gravity of the resulting injury if the threat does materialize, and (3) the burden of implementing adequate precautions.[86] In other words, the standard of care to be exercised in any particular case depends upon the circumstances of that case and on the extent of foreseeable danger.[87]

Security regulations take a similar approach, and indicate that the following factors are relevant in determining what security measures should be implemented in a given case:

- The probability and criticality of potential risks
- The company's size, complexity, and capabilities
- The nature and scope of the business activities
- The nature and sensitivity of the information to be protected
- The company's technical infrastructure, hardware, and software security capabilities
- The state of the art re technology and security
- The costs of the security measures[88]

Interestingly, cost was the one factor mentioned most often, and certainly implies recognition that companies are not required to do everything theoretically possible.

(2) Categories of Security Measures that Must Be Addressed

Specifying a process still leaves many businesses wondering, "What specific security measures should I implement?" In other words, in developing a security plan, what security measures or safeguards should be included?

Generally, the law does not require companies to implement specific security measures or use a particular technology. As expressly stated in the HIPAA security regulations, for example, companies

---

[85] *See, generally,* requirements of FTC Consent Decrees listed in the Appendix.

[86] *See, e.g., United States v. Carroll Towing,* 159 F.2d 169, 173 (2d Cir. 1947).

[87] *See, e.g., DCR Inc. v. Peak Alarm Co.,* 663 P.2d 433, 435 (Utah 1983); *see also Glatt v. Feist,* 156 N.W.2d 819, 829 (N.D. 1968) (the amount or degree of diligence necessary to constitute ordinary care varies with facts and circumstances of each case).

[88] *See, e.g.,* Massachusetts Security regulations, 201 CMR 17.03(1).

"may use any security measures" reasonably designed to achieve the objectives specified in the regulations.[89]

This focus on flexibility means that, like the obligation to use "reasonable care" under tort law, determining compliance may ultimately become more difficult, as there are unlikely to be any safe-harbors for security.

Nonetheless, viewing existing laws, regulations, and security standards as a group suggests that companies consider certain *categories* of security measures, and then decide whether, and in what manner, it should implement security measures to address each category. The general categories of security measures mentioned most often in the various laws, regulations, and security standards include the following:

- **Physical Facility and Device Security Controls** – Procedures to safeguard the facility, measures to protect against destruction, loss, or damage of information due to potential environmental hazards (such as fire and water damage or technological failures), procedures that govern the receipt and removal of hardware and electronic media into and out of a facility, and procedures that govern the use and security of physical workstations.
- **Physical Access Controls** – Access restrictions at buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.
- **Technical Access Controls** – Policies and procedures to ensure that authorized persons who need access to the system have appropriate access, and that those who should not have access are prevented from obtaining access, including procedures to determine access authorization, procedures for granting and controlling access, authentication procedures to verify that a person or entity seeking access is the one claimed, and procedures for terminating access.
- **Intrusion Detection Procedures** – Procedures to monitor log-in attempts and report discrepancies; system monitoring and intrusion detection systems and procedures to detect actual and attempted attacks on or intrusions into company information systems; and procedures for preventing, detecting, and reporting malicious software (e.g., virus software, Trojan horses, etc.);
- **Employee Procedures** – Job control procedures, segregation of duties, and background checks for employees with responsibility for or access to information to be protected, and controls to prevent employees from providing information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- **System Modification Procedures** – Procedures designed to ensure that system modifications are consistent with the company's security program;
- **Data Integrity, Confidentiality, and Storage** – Procedures to protect information from unauthorized access, alteration, disclosure, or destruction during storage or transmission, including storage of data in a format that cannot be meaningfully interpreted if opened as a flat, plain-text file, or in a location that is inaccessible to unauthorized persons and/or protected by a firewall;
- **Data Destruction and Hardware and Media Disposal** – Procedures regarding final disposition of information and/or hardware on which it resides, and procedures for removal from media before re-use of the media;

[89] HIPAA Security Regulations, 45 CFR Section 164.306(b)(1). There are some exceptions, however. For example, the Massachusetts security regulations require implementation of firewalls, the use of virus software, and in certain cases, the use of encryption. See 201 CMR 17.00.

- **Audit Controls** – Maintenance of records to document repairs and modifications to the physical components to the facility related to security (e.g., walls, doors, locks, etc); and hardware, software, and/or procedural audit control mechanisms that record and examine activity in the systems;
- **Contingency Plan** – Procedures designed to ensure the ability to continue operations in the event of an emergency, such as a data backup plan, disaster recovery plan, and emergency mode operation plan;
- **Incident Response Plan** – A plan for taking responsive actions in the event the company suspects or detects that a security breach has occurred, including ensuring that appropriate persons within the organization are promptly notified of security breaches, and that prompt action is taken both in terms of responding to the breach (e.g., to stop further information compromised and to work with law enforcement), and in terms of notifying appropriate persons who may be potentially injured by the breach.

(d) Awareness, Training and Education

Training and education for employees is a critical component of any security program. Newer statutes, regulations, and consent decrees in the United States clearly recognize that even the very best physical, technical, and administrative security measures are of little value if employees do not understand their roles and responsibilities with respect to security. For example, installing heavy duty doors with state of the art locks (whether of the physical or virtual variety), will not provide the intended protection if the employees authorized to have access leave the doors open and unlocked for unauthorized persons to pass through.

Security education begins with communication to employees of applicable security policies, procedures, standards, and guidelines. It also includes implementing a security awareness program, periodic security reminders, and developing and maintaining relevant employee training materials, such as user education concerning virus protection, password management, and how to report discrepancies. Applying appropriate sanctions against employees who fail to comply with security policies and procedures is also important.

(e) Monitoring and Testing

Merely implementing security measures is not sufficient. Companies must also ensure that the security measures have been properly put in place and are effective. This includes conducting an assessment of the sufficiency of the security measures in place to control the identified risks, and conducting regular testing or monitoring of the effectiveness of those measures. Existing precedent also suggests that companies must monitor compliance with its security program. To that end, a regular review of records of system activity, such as audit logs, access reports, and security incident tracking reports is also important.

(f) Review and Adjustment

Perhaps most significantly, the legal standard for information security recognizes that security is a moving target. Businesses must constantly keep up with every changing threats, risks, vulnerabilities, and security measures available to respond to them. It is a never-ending process. As a consequence, businesses must conduct periodic internal reviews to evaluate and adjust the information security program in light of:

- The results of the testing and monitoring
- Any material changes to the business or arrangements
- Any changes in technology
- Any changes in internal or external threats
- Any environmental or operational changes
- Any other circumstances that may have a material impact.

In addition to periodic internal reviews, best practices and the developing legal standard may require that businesses obtain a periodic review and assessment (audit) by qualified independent third-party professionals using procedures and standards generally accepted in the profession to certify that the security program meets or exceeds applicable requirements, and is operating with sufficient effectiveness to provide reasonable assurances that the security, confidentiality, and integrity of information is protected. It should then adjust the security program in light of the findings or recommendations that come from such reviews.

(g) Oversee Third Party Service Provider Arrangements

In today's business environment, companies often rely on third parties, such as outsource providers, to handle much of their data. When corporate data is in the possession and under the control of a third party, this presents special challenges for ensuring security.

Laws and regulations imposing information security obligations on businesses often expressly address requirements with respect to the use of third party outsource providers. First and foremost, they make clear that regardless of who performs the work, the legal obligation to provide the security itself remains with the company. As it is often said, "you can outsource the work, but not the responsibility." Thus, third party relationships should be subject to the same risk management, security, privacy, and other protection policies that would be expected if a business were conducting the activities directly.[90]

Accordingly, the developing legal standard for security imposes three basic requirements on businesses that outsource: (1) they must exercise due diligence in selecting service providers, (2) they must contractually require outsource providers to implement appropriate security measures, and (3) they must monitor the performance of the outsource providers.[91]

4. Special Rules for Specific Data Elements

In addition to laws imposing general security obligations with respect to personal information, developing law is also imposing new obligations to protect specific data elements or sub-categories of personal data. That is, laws, regulations, and standards are beginning to focus on specific data elements, and imposing specific obligations with respect to such data elements. Prime examples include Social Security numbers, credit card transaction data, and other sensitive data.

(a) Sensitive Data

From its inception, the EU Data Protection Directive has required special treatment for particularly sensitive personal information. Specifically, the Directive prohibits "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union

[90] See, e.g., Massachusetts Security Regulations, 201 CMR 17.02(2)(f).

[91] See, e.g., Massachusetts Security Regulations, 201 CMR 17.02(2)(f).

membership, and the processing of data concerning health or sex life," unless certain exceptions apply.[92] Those exceptions include "explicit consent" by the data subject, and carrying out obligations under applicable employment laws.

But even with consent, processing such sensitive data, according to EU interpretation, requires that "special attention" be given to data security aspects to avoid risks of unauthorized disclosure. In particular, "*[a]ccess by unauthorized persons must be virtually impossible and prevented*." [93]

In the United States, a de facto category of sensitive information has been defined by the various state security breach notification laws. These laws require special action (i.e., disclosure) in the event of a breach of security with respect to a subcategory of personal data generally considered to be sensitive because of its potential role in facilitating identity theft.

(b) Social Security Numbers

The security of Social Security numbers has been the particular focus of numerous state laws enacted in recent years (see list in Appendix). The scope of these laws ranges from restrictions on the manner in which Social Security numbers can be used to requirements for security when communicating and/or storing such numbers. For example, several states have enacted laws that prohibit requiring an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the number is encrypted.[94]

(c) Credit Card Data

For businesses that accept credit card transactions, the Payment Card Industry Data Security Standards ("PCI Standards")[95] impose significant security obligations with respect to credit card data captured as part of any credit card transaction. The PCI Standards, jointly created by the major credit card associations, require businesses that accept MasterCard, Visa, American Express, Discover, and Diner's Club cards to comply. At least three states have now incorporated at least part of the PCI Standards in their law.[96]

5. Special Rules for Specific Security Controls

(a) Duty to Encrypt Data

Some laws and regulations impose obligations to use encryption in certain situations. Initially this included state laws that mandate encryption of Social Security numbers for communication over the Internet.[97] More recently, however, some state laws prohibit the electronic transmission of any personal information to a person outside of the secure system of the business (other than a facsimile) unless the

---

[92] EU Data Protection Directive, Article 8.

[93] Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, February 15, 2007, at pp. 19-20; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf (emphasis in original).

[94] *See* list of state laws in GAO Report, Social Security Numbers: Federal and State Laws Restrict Use of SSN's, Yet Gaps Remain, September 15, 2005 at Appendix III; available at www.gao.gov/new.items/d051016t.pdf.

[95] Available at www.pcisecuritystandards.org.

[96] See list in Appendix.

[97] Ariz. Rev. Stat. § 44-1373, Cal. Civ. Code § 1798.85, Conn. Gen. Stat. § 42-470, Md. Commercial Law Code Ann. § 14-3402(4).

information is encrypted.[98] Most notable are the Massachusetts Regulations, which require businesses to encrypt personal information if it is stored on "laptops or other portable devices," "will travel across public networks," or will "be transmitted wirelessly."[99]

(b) Data Destruction

A new trend during the past few years has been for laws and regulations to impose security requirements with respect to the manner in which data is destroyed. These regulations typically do not require the destruction of data, but seek to regulate the manner of destruction when companies decide to do so. These laws also typically apply to the destruction of personal data.

At the Federal level, both the banking regulators and the SEC have adopted regulations regarding security requirements for the destruction of personal data. Similarly, at the State level, at least 19 states have now adopted similar requirements.[100]

Such statutes and regulations generally require companies to properly dispose of personal information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. With respect to information in paper form, this typically requires implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that the information cannot be read or reconstructed. With respect to electronic information, such regulations typically require implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer personal information so that the information cannot practicably be read or reconstructed.[101]

C. THE DUTY TO WARN OF SECURITY BREACHES

In addition to the foregoing legal trend imposing an obligation to *implement* security measures to protect data, we are also witnessing a global trend to enact laws and regulations that impose an obligation to *disclose* security breaches to the persons affected. But unlike laws that impose a duty to provide security, these laws typically require only that companies disclose security breaches to affected persons.[102]

Designed as a way to help protect persons who might be adversely affected by a security breach of their personal information, these laws impose on companies an obligation similar to the common law "duty to warn" of dangers. Such a duty is often based on the view that a party who has a superior knowledge of a danger of injury or damage to another that is posed by a specific hazard must warn those who lack such knowledge. By requiring notice to persons who may be adversely affected by a security breach (e.g., persons whose compromised personal information may be used to facilitate identity theft), these laws seek to provide such persons with a warning that their personal information has been

---

[98] NRS 597.970

[99] 201 CMR 17.04(3) and (5).

[100] See list in Appendix.

[101] See, e.g., 16 CFR Section 682.3.

[102] Pisciotta v. Old National Bancorp., 2007 U.S. App. Lexis 20068 (7th Cir. August 23, 2007), at p. 13.

compromised, and an opportunity to take steps to protect themselves against the consequences of identity theft.[103]

For the most part, laws imposing an obligation to disclose security breaches are a direct reaction to a series of well-publicized security breaches involving sensitive personal information over the past few years,[104] and an effort to address the problem of identity theft. Yet the concept of such laws is not new, nor is it limited to personal information. In 1998, for example, the Internal Revenue Service imposed a disclosure requirement on all taxpayers whose electronic tax records were the subject of a security breach. In a Revenue Procedure that sets forth its basic rules for maintaining tax-related records in electronic form, the IRS requires taxpayers to "promptly notify" the IRS District Director if any electronic tax records "are lost, stolen, destroyed, damaged, or otherwise no longer capable of being processed …, or are found to be incomplete or materially inaccurate."[105]

With respect to personal information, almost all states in the U.S. have now enacted security breach notification laws, all generally based on a 2003 California law.[106] These laws are generally applicable to all businesses that maintain data about residents of the enacting state.

These laws generally require that any business in possession of computerized sensitive personal information about an individual must disclose a breach of the security of such information to the person affected.[107] Sensitive personal information is typically defined as information consisting of: (1) a person's first name or initial and last name, plus (2) any one of the following: social security number, drivers license or state ID number, or financial account number or credit or debit card number (along with any PIN or other access code where required for access to the account). In some states this list is longer, and may also include medical information, insurance policy numbers, passwords by themselves, biometric information, professional license or permit numbers, telecommunication access codes, mother's maiden name, employer ID number, electronic signatures, and descriptions of an individual's personal characteristics.[108] When a triggering event occurs, and the notice requirements themselves, also vary from state-to-state.

1. The Basic Obligation

Taken as a group, the state and federal security breach notification laws generally require that any business in possession of sensitive personal information about a covered individual must disclose any breach of such information to the person affected. The key requirements, which vary from state-to-state, include the following:

---

[103] *See, e.g.*, Recommended Practices on Notice of Security Breach Involving Personal Information, Office of Privacy Protection, California Department of Consumer Affairs, April, 2006 (hereinafter "California Recommended Practices"), at pp. 5-6 (available at www.privacy.ca.gov/recommendations/secbreach.pdf); Interagency Guidance *supra* note 4 , at p. 15752.

[104] For a chronology of such breaches in the U.S., and a running total of the number of individuals affected, see Privacy Rights Clearinghouse at www.privacyrights.org/ar/ChronDataBreaches.htm.

[105] IRS Rev. Proc. 98-25, § 8.01.

[106] See list of statutes in Appendix.

[107] Except where the business maintains computerized personal information that the business does not own or license, in which case the laws require the business to notify the owner of the information, rather than the individuals themselves, of any breach of the security of the system.

[108] *See, e.g.*, Ark. Code § 4-110-101 et seq.; La. Rev. Stat. § 51:3071 et seq.; Md. Code, § 14-3501 et. seq.; Neb. Rev Stat 87-801 et. seq.; N.J. Stat. 56:8-163; N.C. Gen. Stat § 75-65; N.D. Cent. Code § 51-30-01 et seq.; Oregon, 2007 S.B. 583. The Federal banking Interagency Guidance also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

- **Type of information** – The statutes generally apply to unencrypted sensitive personally identified information – e.g., information consisting of first name or initial and last name, plus one of the following: social security number, drivers license or other state ID number, or financial account number or credit or debit card number (along with any PIN or other access code where required for access to the account).
- **Definition of breach** – Generally the statutes require notice following the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of such personal information. In some states, however, notice is not required unless there is a reasonable basis to believe that the breach will result in substantial harm or inconvenience to the customer.
- **Who must be notified** – Notice must be given to any residents of the state whose unencrypted personal information was the subject of the breach.
- **When notice must be provided** – Generally, persons must be notified in the most expedient time possible and without unreasonable delay; however, in most states the time for notice may be extended for the following:
  - ✓ Legitimate needs of law enforcement, if notification would impede a criminal investigation
  - ✓ Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system
- **Form of notice** – Notice may be provided in writing (e.g., on paper and sent by mail), in electronic form (e.g., by e-mail, but only provided the provisions of E-SIGN[109] are complied with), or by substitute notice.
- **Substitute notice options** – If the cost of providing individual notice is greater than a certain amount (e.g., $250,000) or if more than a certain number of people would have to be notified (e.g., 500,000), substitute notice may be used, consisting of:
  - ✓ E-mail when the e-mail address is available, and
  - ✓ Conspicuous posting on the company's web site, and
  - ✓ Publishing notice in all major statewide media.

Several of these issues vary from state to state, however, and some have become controversial. The biggest issue revolves around the nature of the triggering event. In California, for example, notification is required whenever there has been an unauthorized access that compromises the security, confidentiality, or integrity of electronic personal data. In other states, however, unauthorized access does not trigger the notification requirement unless there is a reasonable likelihood of harm to the individuals whose personal information is involved[110] or unless the breach is material.[111]

2. International Adoption

Although the breach notification concept began in the United States, it is rapidly spreading internationally. Currently, countries imposing some sort of duty to notify of security breaches include:

---

[109] 15 USC Section 7001 *et. seq*. This generally requires that companies comply with the requisite consumer consent provisions of E-SIGN at 15 USC Section 7001(c).

[110] Arkansas, Connecticut, Delaware, and Louisiana are examples of states in this category.

[111] Montana and Nevada are examples of states in this category.

- Austria
- Canada (Alberta only)
- Chile
- Denmark
- Finland
- France
- Germany
- Greece
- India
- Ireland
- Italy
- Mexico
- Norway
- Portugal
- Qatar
- Russia
- South Korea

In January 2012 the European Commission also released its proposed General Data Protection Regulation (the "Proposed Regulation").[112] This proposed regulation implements a comprehensive reform of EU data protection laws to strengthen online privacy rights and boost Europe's digital economy.

The proposed Regulation imposes a general requirement on all businesses to notify data protection authorities and data subjects in the event of a data breach. As proposed, notice of data breaches must be provided to the data protection authority "where feasible" within 24 hours, and to affected data subjects "without undue delay." While breach notice has recently become a requirement for telecommunications and internet service providers, the Proposed Regulation extends this requirement to all organisations.

D. PUTTING IT ALL TOGETHER – THE CYBERSECURITY FRAMEWORK

On February 12, 2014, the National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework).[113] Although promoted as a voluntary tool to assist companies in addressing security, the Cybersecurity Framework, which arguably incorporates most of the issues discussed above, may well become the standard for data security for all businesses.

1. Source and Nature of the Framework

The Cybersecurity Framework is one of the deliverables contemplated by the President's Executive Order 13636 on "Improving Critical Infrastructure Cybersecurity" that was released on February 12, 2013.[114] Recognizing that the national and economic security of the United States depends on the reliable functioning of the critical infrastructure that Executive Order directed NIST to work with the private sector to develop a voluntary Framework – based on existing standards, guidelines, and practices -- for reducing cyber risks to the nation's critical infrastructure.

---

[112] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[113] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[114] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Consistent with the requirements of the Executive Order, the Framework was created through collaboration between industry and government,[115] and "provides a consensus description of what's needed for a comprehensive cybersecurity program." "It reflects the efforts of a broad range of industries that see the value of and need for improving cybersecurity and lowering risk."[116] And according to NIST, it "allows organizations—regardless of size, degree of cyber risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure."[117]

The Framework references several generally accepted domestic and international security standards, and is generally agreed by the participants to constitute best practice for cybersecurity.[118] It might be argued that the Framework is little more than a compilation of established industry security practices, but even so, it collates such practices into a framework of activities that arguably establishes a set of requirements for the development of "reasonable" security practices. Moreover, it carries the weight of being a government-issued framework that was the result of a year-long collaboration between industry and government to develop a voluntary "how to" guide for organizations to enhance their cybersecurity.[119]

Technically, the Cybersecurity Framework was written only for businesses in the 16 critical infrastructure sectors.[120] But the practical reality goes much farther. The Framework is written as a generally applicable document that is in no way unique to critical infrastructure industries. It is not industry-specific, nor is it country-specific. And consistent with existing law, the Framework adopts a risk-based approach to managing cybersecurity risk. As such, it appears to fit quite well with the approach of existing legal requirements for cybersecurity obligations. It provides generic approaches and activities to address cybersecurity for all businesses.

The Framework is also designed to be technology neutral. It relies on a variety of existing standards, guidelines, and practices, most of which are internationally recognized. Thus, it should be able to scale across borders and evolve with technological advances and business requirements.

Created through collaboration between government and the private sector, the Framework uses a common and simplified language to address and manage cybersecurity risk. It provides a common language for understanding, managing, and expressing cybersecurity risk, and thus provides a non-technical tool for aligning policy, business and technological approaches to managing risk.

---

[115] The "framework is the culmination of a year-long effort that brought together thousands of individuals and organizations from industry, academia and government." Press release "NIST Releases Cybersecurity Framework Version 1.0," February 12, 2014, available at http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

[116] Statement by Under Secretary of Commerce for Standards and Technology and NIST Director Patrick D. Gallagher, cited in press release "NIST Releases Cybersecurity Framework Version 1.0," February 12, 2014, available at http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

[117] Id.

[118] "Over the past year, individuals and organizations throughout the country and across the globe have provided their thoughts on the kinds of standards, best practices, and guidelines that would meaningfully improve critical infrastructure cybersecurity. The Department of Commerce's National Institute of Standards and Technology (NIST) consolidated that input into the voluntary Cybersecurity Framework that we are releasing today." White House Press Release, Launch of the Cybersecurity Framework, February 12, 2014, available at http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework.

[119] http://www.nist.gov/cyberframework

[120] According to Presidential Policy Directive 21 (PPD-21), the 16 critical infrastructure sectors are: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation, and water and waste water systems.

The Framework does not actually create standards in the normal sense of that word. Rather, it creates a standardized approach – a process – for companies to identify, describe, address, and communicate their cybersecurity measures and risks. In doing so, the Framework provides organization and structure to the multiple existing approaches to cybersecurity by assembling references to standards, guidelines, and practices that are working effectively in industry today. Most of those standards are internationally recognized. Thus, the Framework provides guidance to an organization on how to manage its cybersecurity risk.

The framework allows organizations—regardless of size, degree of cyber risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.[121]

At present, however, the Cybersecurity Framework has no legal standing. It is neither a law nor a regulation, and thus does not impose on any business a legal duty to provide data security or constitute a legally-binding standard to follow. Yet it may well become the legal standard for defining reasonable security in the near future.

A key question for businesses outside of the critical infrastructure sectors is whether the Cybersecurity Framework applies to them. And a key question for all business in all sectors, is whether, or to what extent, the "voluntary" Cybersecurity Framework will constitute a legally-recognized best practice or some sort of a binding legal definition of reasonable security that will be either (1) used to assess liability for failure to implement appropriate security, or (2) provide a safe harbor for security compliance.

2. Summary of the Framework

The Framework consists of 3 parts, referred to as the Framework Core, the Framework Profiles, and the Framework Tiers, described as follows:

- The **Framework Core** is a set of cybersecurity activities and informative references that are common across critical infrastructure sectors. The cybersecurity activities are grouped by five functions -- Identify, Protect, Detect, Respond, Recover -- that provide a high-level view of an organization's management of cyber risks. Taken together, these five functions allow any organization to understand and shape its cybersecurity program.
- The **Framework Profiles** can help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources. Companies can use the Profiles to understand their current cybersecurity state, support prioritization, and to measure progress towards a target state. The profiles help organizations progress from a current level of cybersecurity sophistication to a target improved state that meets business needs.
- The **Framework Tiers** provide a mechanism for organizations to view their approach and processes for managing cyber risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor in risk management practices, the extent to which cybersecurity risk management is informed by business needs, and its integration into an organization's overall risk management practices. The tiers describe the degree to which an organization's cybersecurity risk management meets goals set out in the Framework.

[121] See press release "NIST Releases Cybersecurity Framework Version 1.0," February 12, 2014, available at http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

Each of the Framework components (the Core, Profiles, and Tiers) reinforces the connection between business drivers and cybersecurity activities. The Framework also offers guidance regarding privacy and civil liberties considerations that may result from cybersecurity activities. From the perspective of defining reasonable security however, the Framework Core is the critical part.

(a) Framework Core

The Framework Core provides a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. Essentially it provides a common set of activities for managing cybersecurity risk, and references specific standards and other forms of guidance to achieve those outcomes. Those activities cover five core functions labelled as: identify, protect, detect, respond, and recover.

The activities of the Framework core are designed to be flexible, and to provide a roadmap for business seeking to address cybersecurity requirements. And they reinforce the view that data security is a relative concept. Thus, the Framework core does not specify particular security measures that a business must implement. There are no references anywhere in the document to familiar security measures such as firewalls, encryption, passwords, or antivirus tools. Rather, the Framework sets out a process that a business should follow to determine how to address its own unique cybersecurity needs. It is an approach similar in concept to the requirement for a written information security program (a so-called WISP) required be some regulations, but goes much farther.

Unlike the WISP rules, which tend to be written as requirements for compliance, the Framework core is written in terms of outcomes. That is, rather than requiring companies to take certain actions, such as conducting a risk assessment by identifying vulnerabilities, identifying threats, and assessing their impact (as a WISP requires), the Framework Core focuses on outcomes, and thus asks whether vulnerabilities have been identified, threats have been identified, and the resulting impact has been assessed. It would seem, however, that in terms of a roadmap or standard for corporate compliance, the result is essentially the same. Most importantly, because the Framework essentially incorporates all of the elements of the WISP concept, and is consistent with the process-oriented risk-based approach of the WISP, it may well become the standard of care going forward.

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a written as a checklist of actions to perform. Instead it presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk. But the net effect may be the same

The activities outlined by the Framework core set forth, at a very high level, activities that are likely to come to be viewed as basic requirements (i.e., best practices) for the data security processes businesses should be following. The level of detail starts at the very general (Functions), progresses to more detail (Categories within Functions), and then ultimately to the lowest of the three levels of detail (Subcategories within Categories). Those five Functions and their respective Categories and Subcategories can be summarized as follows:

Identify Function. This function involves developing the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. It is fundamental to all data security activities, and includes the following Categories:

- Asset Management Category: Identification of all assets to be protected (physical devices, software, data flows, etc.);

- Business Environment Category: Identification of business environment, including the organizations role in the supply chain and critical infrastructure;
- Governance Category: Identification of governance policies, procedures and processes to manage and monitor the entity's regulatory, legal, risk, environmental, and operational requirements;
- Risk Assessment Category: Risk assessment – *i.e.*, identification of the threats, vulnerabilities, and impact thereof on the organization;
- Risk Management Strategy Category: Identification of risk management strategy – *i.e.*, the organizations priorities, constraints, risk tolerances, and assumptions.

Protect Function. Once the assets to be protected and the risks they face have been identified, the next step is to put in place the processes, procedures, and security measures to provide such protection – *i.e.*, to implement appropriate safeguards. This includes the following categories:

- Access Control Category: Access control processes and procedures should limit access to processes, devices, and data to authorized users;
- Awareness and Training Category: Appropriate education and training should be provided for employees and business partners regarding security-related duties and responsibilities;
- Data Security Category: Security measures, processes, and procedures should be implemented to protect data at rest, data in transit, data integrity and to protect against data leaks;
- Information Protection Processes and Procedures Category: Security measures should be implemented to manage the protection of information systems and assets;
- Maintenance Category: Address maintenance and repairs of control systems and information system components consistent with policies and processes;
- Protective Technology Category: Manage technical security solutions to ensure the security and resilience of systems and assets (e.g., audit logs, removable media, and communications & control networks).

Detect Function. Processes, procedures, and policies should be in place to detect the occurrence of cybersecurity events. These include the following categories:

- Anomalies and Events Category: The ability to detect anomalous activities in a timely manner and understand the potential impact of events;
- Security Continuous Monitoring Category: Continuous security monitoring of information systems and assets to identify cybersecurity events and verify the effectiveness of protective measures;
- Detection Processes Category: and procedures to ensure timely and adequate awareness of anomalous events.

Respond Function. Processes and procedures should be in place to properly and promptly respond to detected cybersecurity events. These include the following:

- Response Planning Category: Implement response processes and procedures designed to ensure timely response to detected cybersecurity events;
- Communications Category: Coordinate response activities with internal and external stakeholders, including law enforcement agencies;
- Analysis Category: Ensure adequate analysis (including forensics) is conducted to ensure adequate response and support recovery activities;
- Mitigation Category: Perform activities to prevent expansion of an event, mitigate its effects, and eradicate the incident; and
- Improvement Category: Ensure that organizational response activities are improved to incorporate lessons learned from current and previous detection/response activities.

Recover Function. Processes and procedures should be in place to recover from security incidents, and to restore any capabilities or services that were impaired. These include the following:

- Recovery Planning Category: Ensure execution of recovery processes and procedures to ensure timely restoration of systems affected by cybersecurity events;
- Improvements Category: Recovery planning and processes should be improved by incorporating lessons learned;
- Communications Category: Restoration activities should be coordinated with internal and external parties.

As one commentator noted, the Framework "doesn't tell companies what to do or what tools to buy, but it does standardize the questions all CEO's should ask about their company's security practices as well as those of their suppliers, partners, and customers. And it shows them what the answers ought to look like."[122] Thus, there is a good possibility that the Framework will become the *de facto* standard for private sector cybersecurity in the eyes of U.S. lawyers and regulators.

Although not a perfect one-to-one match, it appears that the requirements of the WISP are essentially covered by the Identify and Protect activities of the Core. However it can also be argued that many of the requirements of the Detect, Respond, and Recover activities of the Framework should be addressed by the security measures adopted pursuant to the WISP process as well.

(b) Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. In essence, they describe the state of an organization's adoption of the Framework.

The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. The four implementation tiers are:

- Tier 1: Partial: Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established.
- Tier 2 Risk informed: Risk management practices are approved by management but may not be established as organizational-wide policy. There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established.
- Tier 3 Repeatable: The organization's risk management practices are formally approved and expressed as policy. There is an organization-wide approach to manage cybersecurity risk.
- Tier 4 Adaptive: The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. There is an

[122] Why Businesses Can't Ignore US Cybersecurity Framework, InformationWeek, February 14, 2014, available at http://www.informationweek.com/government/cybersecurity/why-businesses-cant-ignore-us-cybersecurity-framework/d/d-id/1113838.

organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.

(c) Framework Profile

The Framework Profile ("Profile") is the alignment by each business of the Functions, Categories, and Subcategories with its own requirements, risk tolerance, and resources. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Each business should develop its own Framework Profiles to describe the current state and then the desired target state of its specific cybersecurity activities. The Current Profile of a business indicates the cybersecurity outcomes described in the Core that are currently being achieved. The Target Profile of a business indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in the communication of risk within and between organizations.

A comparison of a company's Current Profile with its Target Profile may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps can contribute to the roadmap described above. Prioritization of gap mitigation is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner.

3. Using the Framework

"The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program."[123] The drafters of the Framework contemplate that "Organizations can use the framework to determine their current level of cybersecurity, set goals for cybersecurity that are in sync with their business environment, and establish a plan for improving or maintaining their cybersecurity. It also offers a methodology to protect privacy and civil liberties to help organizations incorporate those protections into a comprehensive cybersecurity program."[124]

[123] Cybersecurity Framework at p. 13. See generally Framework Section 3.2 "Establishing or Improving a Cybersecurity Program," at pp. 13-15.

[124] See press release "NIST Releases Cybersecurity Framework Version 1.0," February 12, 2014, available at http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

APPENDIX

Key Information Security Law References

A. Federal Statutes

1. **COPPA**: Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 *et seq*.
2. **E-SIGN**: Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001(d).
3. **FCRA/FACTA:** Fair Credit Reporting Act,
4. **FISMA**: Federal Information Security Management Act of 2002, 44 U.S.C. Sections 3541-3549.
5. **FTC Act:** Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), prohibits unfair or deceptive acts or practices in or affecting commerce.
6. **GLB Act**: Gramm-Leach-Bliley Act, Public L. 106-102, Sections 501 and 505(b), 15 U.S.C. Sections 6801, 6805.
7. **HIPAA**: Health Insurance Portability and Accountability Act, 42 U.S.C. 1320d-2 and 1320d-4. See also Subtitle D of Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), at sections 13401 *et. seq.*
8. **Homeland Security Act of 2002**: 44 U.S.C. Section 3532(b)(1).
9. **Privacy Act of 1974:** 5 U.S.C. Section 552a
10. **Sarbanes-Oxley Act**: Pub. L. 107-204, Sections 302 and 404, 15 U.S.C. Sections 7241 and 7262.
11. **Federal Rules of Evidence 901(a):** *see American Express v. Vinhnee*, 2005 Bankr. LEXIS 2602 (9th Cir. Bk. App. Panel, 2005), and *Lorraine v. Markel*, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007).

B. State Statutes

1. **UETA**: Uniform Electronic Transaction Act, Section 12 (now enacted in 47 states).
2. **Law Imposing Obligations to Provide Security for Personal Information**:

Arkansas	Ark. Code Ann. § 4-110-104(b)
California	Cal. Civ. Code § 1798.81.5(b)
Connecticut	Conn. Gen. Stat. § 42-471
Illinois	740 Ill. Comp. Stat. Ann. 14/1 (Biometric Information Privacy Act)
Maryland	Md. Com. Law Code Ann. § 14-3503
Massachusetts	Mass. Gen. Laws. Ch. 93H, § 2(a); Regulations at 201 CMR 17.00 et. seq.
Nevada	Nev. Rev. Stat. 603A.210
New Jersey	N.J.A.C. 13:45F-3 (Pre-Proposed New Rules – 12/15/08)
Oregon	Or. Rev. Stat. Section 646A.622
Rhode Island	R.I. Stat. 11-49.2-2(2) and (3)
Texas	Tex. Bus. & Com. Code Ann. § 521.052
Utah	Utah Code Ann. § 13-44-201

3. **Law Imposing Obligations to Provide Security for Credit Card Information**:

Minnesota	Minn. Stat. Chapter 325E.64
Nevada	Nev. Rev. Stat. 603A.215
Washington	RCWA Chapter 19.255

4. **Law Imposing Duty to Encrypt Personal Information**:

Arizona	Ariz. Rev. Stat. § 44-1373
California	Cal. Civil Code Section 1798.85(a)(3) [SSN]
Connecticut	Conn. Gen. Stat. § 42-470
Maryland	Md. Comm. Code § 14-3302(a)(3) [SSN]
Massachusetts	Mass. Gen. Laws. Ch. 93H, § 2(a); Regulations at 201 CMR 17.00 et. seq. [Personal Information on laptops, etc]
Nevada	Nev. Rev. Stat. 603A.215

5. **Data Disposal / Destruction Laws**:

Alaska	Ala. Stat. §§ 45.48.500 – 45.48.590
Arkansas	Ark. Code Ann. § 4-110-104(a)
California	Cal. Civil Code § 1798.81.
Connecticut	Conn. Gen. Stat. § 42-471
Georgia	Ga. Stat § 10-15-2
Hawaii	Haw. Stat Section § 487R-2
Illinois	815 ILCS 530/40 (all);
Indiana	Ind. Code § 24-4-14
Kentucky	Ken. Rev. Stat. § 365.720
Maryland	Md. Code, § 14-3502; Md. HB 208 & SB 194
Massachusetts	Mass. Gen. laws. Ch. 93I
Michigan	MCL § 445.72a
Montana	Mont. Stat. § 30-14-1703
Nevada	Nev. Rev. Stat. 603A.200
New Jersey	N.J. Stat. 56:8-162
North Carolina	N.C. Gen. Stat § 75-64
Oregon	2007 S.B. 583, Section 12
Texas	Tex. Bus. & Com. Code Ann. § 48.102(b)
Utah	Utah Code Ann. § 13-42-201
Vermont	Vt. Stat. Tit. 9 § 2445 et seq.
Washington	RCWA 19.215.020

6. **Security Breach Notification Laws**

Alabama	[No Statute]
Alaska	Ala. Stat. §§ 45.48.010 – 45.48.090
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 et seq.
California	Cal. Civ. Code § 1798.82
Colorado	Col. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. 36A-701(b)
Delaware	De. Code tit. 6, § 12B-101 et seq.
District of Columbia	DC Code § 28-3851 *et seq*.
Florida	Fla. Stat. § 817.5681

Georgia	Ga. Code § 10-1-910 et seq. [125]
Hawaii	Hawaii Rev. Stat. § 487N-2
Idaho	Id. Code §§ 28-51-104 to 28-51-107
Illinois	815 Ill. Comp. Stat. 530/1 et seq.
Indiana	Ind. Code § 24-4.9
Iowa	Iowa Code § 715C.2
Kansas	Kansas Stat. 50-7a01, 50-7a02 (2006 S.B. 196, Chapter 149)
Kentucky	[No Statute]
Louisiana	La. Rev. Stat. § 51:3071 et seq.
Maine	Me. Rev. Stat. tit. 10 §§ 1347 et seq.
Maryland	Md. Code, §§ 14-3501 thru 14-3508;
Massachusetts	Mass. Gen. Laws. Ch. 93H;
Michigan	MCL 445.72
Minnesota	Minn. Stat. § 325E.61, § 609.891
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. Section 407.1500
Montana	Mont. Code § 30-14-1701 et seq.
Nebraska	Neb. Rev Stat 87-801 et. seq.
Nevada	Nev. Rev. Stat. § 603.220
New Hampshire	N.H. RS 359-C:19 et seq.
New Jersey	N.J. Stat. 56:8-163
New Mexico	[No Statute]
New York	N.Y. Bus. Law § 899-aa
North Carolina	N.C. Gen. Stat § 75-65
North Dakota	N.D. Cent. Code § 51-30-01 et seq.
Ohio	Ohio Rev. Code § 1349.19
Oklahoma	Okla. Stat. Tit. 24, § 161, et. seq.
Oregon	Oregon: ORS § 646A
Pennsylvania	73 Pa. Cons. Stat. § 2303
Puerto Rico	P.R. Laws Ann. tit. 10, § 4052
Rhode Island	R.I. Gen. Laws § 11-49.2-1 et seq.
South Carolina	S.C. Code § 39-1-90
South Dakota	[No Statute]
Tennessee	Tenn. Code § 47-18-2107
Texas	Tex. Bus. & Com. Code § 521.053
Utah	Utah Code § 13-44-101 et seq.
Vermont	Vt. Stat. Tit. 9 § 2430 et seq.
Virgin Islands (US)	14 V.I.C. § 2209
Virginia	Va. Code. 18.2-186.6
Washington	Wash. Rev. Code § 19.255.010
West Virginia	W. Va. Code §§46A-2A-101 – 46A-2A-105
Wisconsin	Wis. Stat. § 134.98
Wyoming	Wyo. Stat. §§ 40-12-501 – 40-12-502

[125] Applies to information brokers only.

7. **State SSN Laws**

Alaska	Ala. Stat. §§ 45.48.400 – 45.48.480
Arizona	Ariz. Rev. Stat. § 44-1373
Arkansas	Ark. Code Ann. § 4-86-107; § 6-18-208
California	Cal. Civ. Code § 1798.85; Cal. Fam. Code § 2024.5
Colorado	Colo. Rev. Stat. § 6-1-715; Colo. Rev. Stat. §13-21-109.5; Colo. Rev. Stat. § 23-5-127; Colo. Rev. Stat. § 24-72.3-102;
Connecticut	Conn. Gen. Stat. § 42-470; Conn. Gen. Stat. § 8-64b
Delaware	Del. Code Ann., tit. 7 § 503
Florida	Fla. Stat. ch. 97.0585
Georgia	Ga. Code Ann. § 50-18-72; O.C.G.A. § 10-1-393.8
Guam	5 GCA § 32704; 5 GCA § 32705
Hawaii	Haw. Rev. Stat. § 12-32; Haw. Rev. Stat. § 487J-2; Haw. Rev. Stat. § 12-3
Illinois	815 Ill. Comp. Stat. 505/2QQ; § 815 ILCS 505/2RR
Indiana	Ind. Code § 4-1-10-1 et seq.; Ind. Code § 9-24-6-2; Ind. Code § 9-24-9-2; Ind. Code § 9-24-11-5; Ind. Code § 9-24-16-3; Ind. Code § 4-1-8-5
Kansas	K.S.A. § 75-3520
Louisiana	La. Rev. Stat. Ann. § 17:440; La. Rev. Stat. Ann. § 18:154; La. Rev. Stat. Ann. § 32:409.1; La. Rev. Stat. Ann. § 37:23; La. Rev. Stat. Ann. § 44:11 ; La. Civ. Code § 3352
Maine	10 M.R.S. § 1272-B
Maryland	Md. Code Ann., Com. Law § 14-3402.
Massachusetts	Mass. Gen. Laws Ch. 167B, § 14 & § 22
Michigan	Mich. Comp. Laws § 445.81 et seq..
Minnesota	Minn. Stat. § 325E.59
Mississippi	Miss. Code Ann. § 25-1-111
Missouri	Mo. Rev. Stat. § 407.1355
Montana	Mont. Code Ann. § 32-6-306; Mont. Code § 30-14-1702, § 30-14-1703
Nebraska	Neb. Rev. Stat. § 48-237
Nevada	Nev. Rev. Stat. Chapter 239; Nev. Rev. Stat. Chapter 239B.030; Chapter 239B; Chapter 603
New Jersey	N.J. Stat. Ann. § 47:1-16; N.J. Stat. Ann. § C.56:8-164
New Mexico	N.M. Stat. Ann. § 57-12B-1 et seq.
New York	N.Y. Gen. Bus. Law § 399-dd
North Carolina	N.C. Gen. Stat. § 75-62
North Dakota	N.D. Cent. Code § 39-06-14
Oklahoma	Okla. Stat. tit. 40, § 173.1
Oregon	Or. Rev. Stat. § 107.840
Pennsylvania	74 Pa. Stat. Ann. §§ 201 to 204
Rhode Island	R.I. Gen. Laws § 6-13-17 and § 6-13-19
South Carolina	S.C. Code Ann. § 7-5-170; S.C. Code § 37-20-180
South Dakota	S.D. Codified Laws § 32-12-17.10; S.D. Codified Laws § 32-12-17.13
Texas	Tex. Bus. & Com. Code Ann. 35.48; Tex. Bus. & Com. Code Ann. 35.58; Tex. Elec. Code Ann. § 13.004; Tex. Bus. & Com. Code § 20.02
Utah	Utah Code Ann. § 31A-21-110
Vermont	9 V.S.A. § 2440; 2030
Virginia	Va. Code Ann. § 2.2-3808; Va. Code Ann. § 59.1-443.2
Washington	Rev. Code Wash. (ARCW) § 19.146.205
West Virginia	W. Va. Code § 17E-1-11
Wisconsin	Wis. Stat. § 36.32

8. **State SSN Laws Requiring SSN Policies**

Connecticut	H.B 5658
Michigan	Mich. Comp. Laws Section 445.84
New Mexico	N.M. Stat. Sections 57-12B-2-57-12B-3
New York	NY Gen. Bus. Law Section 3990dd(4)
Texas	Texas Bus. & Com. Code Sections 35.581 (effective through March 31, 2009)

C. Federal Regulations

1. **Regulations Imposing Obligation to Provide Security**

(a) **COPPA Regulations**: 16 C.F.R. 312.8.

(b) **DHS Regulations:** Electronic Signature and Storage of Form I-9, Employment Eligibility Verification, 8 C.F.R. Part 274a (e), (f), (g), and (h).

(c) **FCC Order re Pretexting**, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at Paragraphs 33-36; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf

(d) **FDA Regulations:** 21 C.F.R. Part 11.

(e) **FFIEC Guidance:** Authentication in an Internet Banking Environment , October 12, 2005, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. See also "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment," August 8, 2006 at p. 5, available at http://www.ncua.gov/letters/2006/CU/06-CU-13_encl.pdf; and Supplement to Authentication in an Internet Banking Environment, available at http://www.fdic.gov/news/news/press/2011/pr11111a.pdf.

(f) **GLB Security Regulations**: Interagency Guidelines Establishing Standards for Safeguarding Consumer Information (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 570 (Office of Thrift Supervision), and 16 C.F.R. Part 314 (FTC).

(g) **GLB Security Regulations (FTC)**: FTC Safeguards Rule (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 16 C.F.R. Part 314 (FTC).

(h) **HIPAA Security Regulations**: Final HIPAA Security Regulations, 45 C.F.R. Part 164.

(i) **IRS Regulations**: Rev. Proc. 97-22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25.

(j) **IRS Regulations**: IRS Announcement 98-27, 1998-15 I.R.B. 30, and Tax Regs. 26 C.F.R. § 1.1441-1(e)(4)(iv).

(k) **SEC Guidance:** SEC CF Disclosure Guidance: Topic No. 2, Cybersecurity; http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

(l) **SEC Regulation S-P:** 17 C.F.R. § 248.

(m) **SEC Regulations**: 17 C.F.R. 240.17a-4, and 17 C.F.R. 257.1(e)(3).

(n) **SEC Regulations**: 17 C.F.R. § 248.30 Procedures to safeguard customer records and information; disposal of consumer report information (applies to any broker, dealer, and investment company, and every investment adviser registered with the SEC).

2. Regulations Imposing Authentication Requirements

(a) **ACH Operating Rules** (2005) Section 2.10.2.2 ("Verification of Receiver's Identity")

(b) Banking Know Your Customer Rules

i. 31 CFR § 103.121, Customer Identification Programs for banks, savings associations, credit unions, and certain non-Federally regulated banks

ii. 31 CFR § 103.122, Customer identification programs for broker-dealers

iii. 31 CFR § 103.123, Customer identification programs for futures commission merchants and introducing brokers

iv. 31 CFR § 103.131, Customer identification programs for mutual funds

(c) **FCC Order re Pretexting**, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at Paragraphs 13-25; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf

(d) **FFIEC Guidance**: Authentication in an Internet Banking Environment , October 12, 2005, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. See also and Supplement to Authentication in an Internet Banking Environment, available at http://www.fdic.gov/news/news/press/2011/pr11111a.pdf.

(e) USA PATRIOT Act

i. 31 U.S.C. 5318 – Section 326 – "Verification of Identification"

ii. Know your customer rules

(f) State Credit Freeze laws

(g) UN Convention on the Use of Electronic Communications in International Contracts – Article 9

3. Data Disposal / Destruction Regulations

(a) **FCRA Data Disposal Rules**: 12 C.F.R. Parts 334, 364

(b) **SEC Regulations**: 17 C.F.R. § 248.30 Procedures to safeguard customer records and information; disposal of consumer report information (applies to any broker, dealer, and investment company, and every investment adviser registered with the SEC).

4. Security Breach Notification Regulations

(a) **FCC Order re Pretexting**, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at paragraphs 26-32; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf

(b) **GLB Security Breach Notification Rule**: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. Part 30 (OCC), 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), available at http://ithandbook.ffiec.gov/media/resources/3488/ots-ceo-ltr-214.pdf.

(c) **IRS Regulations**: Rev. Proc. 97-22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25.

(d) **HIPAA Amendments:** Subtitle D of Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), at sections 13401 *et. seq*

(e) **SEC Guidance:** SEC CF Disclosure Guidance: Topic No. 2, Cybersecurity; http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

D. State Regulations

1. **Insurance – NAIC Model Regulations**: National Association of Insurance Commissioners, Standards for Safeguarding Consumer Information, Model Regulation.
2. **Attorneys** – New Jersey Advisory Committee on Professional Ethics, Opinion 701 (2006) available at http://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf

F. Court Decisions

1. *In re: Sony Gaming Networks and Customer Data Security Breach Litigation*, 2014 BL 15530, (S.D. Cal., No. 3:11-md-02258-AJB-MDD, partially dismissed Jan 21, 2014), at pp. 21-22 (recognizing legal duty to provide security).
2. *Lone Star National Bank v Heartland Payment Systems*, No. 12-20648 (5th Cir, Sept. 3, 2013) (recognizing negligence claim and finding economic loss doctrine not applicable)
3. *Cooney v. Chicago Public Schools*, 2010 Ill. App. LEXIS 1424 (December 30, 2010) (no common law duty to provide security)
4. *Prudential Ins. Co. of Am. v. Dukoff*, No. 07-1080, 2009 U.S. Dist. LEXIS 117843 (E.D.N.Y. December 18, 2009) (must authenticate identity of signer of insurance application in order to enforce signature)
5. *Kerr vs. Dillard Store Services, Inc*., 2009 U.S. Dist. Lexis 11792 (D. Kan. Feb 17, 2009) (electronic signature not enforceable due to lack of security re attribution of signer to signature)
6. *In Re TJX Companies Retail Security Breach Litigation*, 2007 U.S. Dist. Lexis 77236 (D. Mass. October 12, 2007) (rejecting a negligence claim due to the economic loss doctrine, but allowing a negligent misrepresentation claim to proceed)
7. *Wolfe v. MBNA America Bank*, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007)
8. *Lorraine v. Markel*, 241 F.R.D. 534, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007)
9. *Guin v. Brazos Higher Education Service*, 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006)
10. *American Express v. Vinhnee*, 336 B.R. 437; 2005 Bankr. LEXIS 2602 (9th Cir. December 16, 2005).
11. *Bell v. Michigan Council 25*, No. 246684, 2005 Mich. App. LEXIS 353 (Mich. App. Feb. 15, 2005) (Unpublished opinion)

12. *Inquiry Regarding the Entry of Verizon-Maine Into The InterLATA Telephone Market Pursuant To Section 271 of Telecommunication Act of 1996*, Docket No. 2000-849, Maine Public Utilities Commission, 2003 Me. PUC LEXIS 181, April 30, 2003; available at http://www.steptoe.com/assets/attachments/1670.pdf

G. FTC Decisions and Consent Decrees

1. FTC v. Wyndham Worldwide Corp., 2014 U.S. Dist. LEXIS 47622 (D. N.J., April 7, 2014) (upholding FTC authority to enforce data security requirements via the FTC Act Section 5 prohibition of unfair business practices).

2. In the Matter of Accretive Health, Inc., FTC File No. 122 3077 (Agreement containing Consent Order, February 24, 2014), available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/122-3077/accretive-health-inc

3. In the Matter of TRENDnet, Inc., FTC File No. 122 3090 (Agreement containing Consent Order, February 7, 2014), available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2013/09/trendnet-inc

4. In the Matter of GMR Transcription Services, Inc., FTC File No. 122 3095 (Agreement containing Consent Order, January 31, 2014), available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/122-3095/gmr-transcription-services-inc-matter

5. In the Matter of CBR Systems, FTC File No. 112 3120 (Decision and Order, May 3, 2013), available at http://www.ftc.gov/os/caselist/1123120/index.shtm

6. In the Matter of HTC America Inc, File No. 122 3049 (Agreement Containing Consent Order, February 22, 2013), available at http://www.ftc.gov/os/caselist/1223049/index.shtm (company failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk)

7. In the Matter of CBR Systems, Inc., FTC File No. 112 3120 (Agreement Containing Consent Order, January 26, 2013), available at http://ftc.gov/os/caselist/1123120

8. FTC v. Wyndham Hotels, (PENDING Lawsuit filed 6/26/2012 http://www.ftc.gov/opa/2012/06/wyndham.shtm)

9. United States of America (For the Federal Trade Commission) v. RockYou, Inc., Case No. 3:12-cv-01487-SI, ND Cal. (Consent Decree and Order, March 27, 2012); available at http://www.ftc.gov/os/caselist/1023120/index.shtm

10. In the Matter of Upromise, Inc., File No 102 3116 (Agreement Containing Consent Order, January 5, 2012), available at http://www.ftc.gov/os/caselist/1023116/index.shtm

11. In the Matter of Facebook, Inc., File No 092 3184 (Agreement Containing Consent Order, November 29, 2011), available at http://ftc.gov/os/caselist/0923184/index.shtm.

12. In the Matter of Twitter, Inc., FTC File No. 092 3093 (Agreement Containing Consent Order, June 24, 2010; Decision and Order, March 11, 2011), available at http://www.ftc.gov/os/caselist/0923093a/index.shtm

13. In the Matter of SettlementOne Credit Corporation, and Sackett National Holdings, Inc., File No. 082 3208 (Agreement Containing Consent Order, February 3, 2011), available at http://www.ftc.gov/os/caselist/0823208/index.shtm

14. In the Matter of ACRAnet, Inc., File No. 092 3088 (Agreement Containing Consent Order, February 3, 2011), available at http://www.ftc.gov/os/caselist/0923088/index.shtm

15. In the Matter of Fajilan and Associates, Inc., also d/b/a Statewide Credit Services, File No. 092 3089 (Agreement Containing Consent Order, February 3, 2011), available at http://www.ftc.gov/os/caselist/0923089/index.shtm

16. In the Matter of Dave & Buster's, Inc., FTC File No. 082 3153 (Agreement Containing Consent Order, March 25, 2010), available at http://www.ftc.gov/os/caselist/0823153/index.shtm

17. United States of America (for the Federal Trade Commission) v. ChoicePoint Inc., FTC File No. 052-3069, (Supplemental Stipulated Judgment and Order For Permanent Injunction and Monetary Relief, October 19, 2009), available at www.ftc.gov/os/caselist/choicepoint/choicepoint.shtm

18. In the Matter of Sears Holdings Management Corporation, FTC File No. 082 3099 (Agreement Containing Consent Order, September 9, 2009), available at http://www.ftc.gov/os/caselist/0823099/index.shtm.

19. U.S. v. Rental Research Services, Inc., FTC File No. 072 3228, D. Minn. (Stipulated Final Judgment, March 5, 2009), available at www.ftc.gov/os/caselist/0723228 [Settlement of allegations that its lack of reasonable client identification procedures and adequate data security safeguards resulted in the sale of credit reports to identity thieves].

20. In the Matter of CVS Caremark Corporation, FTC File No. 072-3119 (Agreement Containing Consent Order, February 18, 2009), available at www.ftc.gov/os/caselist/0723119

21. In the Matter of Genica Corporation, and Compgeeks.com, FTC File No. 082-3113 (Agreement Containing Consent Order, February 5, 2009), available at www.ftc.gov/os/caselist/0823113

22. In the Matter of Premier Capital Lending, Inc., FTC File No. 072-3004 (Agreement Containing Consent Order, November 6, 2008), available at www.ftc.gov/os/caselist/0723004

23. In The Matter of The TJX Companies, Inc., FTC File No. 072-3055 (Agreement Containing Consent Order, March 27, 2008), available at www.ftc.gov/os/caselist/0723055

24. In the Matter of Reed Elsevier Inc. and Seisint, Inc., FTC File No. 052-3094 (Agreement Containing Consent Order, March 27, 2008), available at www.ftc.gov/os/caselist/0523094

25. U.S. v. ValueClick, Inc., Case No. CV08-01711 MMM (RZx), FTC File Nos. 072-3111 and 072-3158 (Stipulated Final Judgment, C.D. Cal. Mar. 17, 2008), available at www.ftc.gov/os/caselist/0723111

26. In the Matter of Goal Financial LLC (Agreement Containing Consent Order, FTC File No. 072 3013, March 4, 2008), available at www.ftc.gov/os/caselist/0723013 [for alleged failure to provide "reasonable and appropriate security" for consumers' personal information in violation of the FTC's Standards for Safeguarding Customer Information Rule and its Privacy of Customer Financial Information Rule (both of which implement provisions of the Gramm-Leach-Bliley Act)]

27. In the Matter of Life is good, Inc. (Agreement Containing Consent Order, FTC File No. 072 3046, January 17, 2008), available at www.ftc.gov/os/caselist/0723046

28. In the Matter of Guidance Software (Agreement Containing Consent Order, FTC File No. 062 3057, November 16, 2006), available at www.ftc.gov/opa/2006/11/guidance.htm

29. In the Matter of CardSystems Solutions, Inc., (Agreement Containing Consent Order, FTC File No. 052 3148, February 23, 2006), *available at* www.ftc.gov/opa/2006/02/cardsystems_r.htm

30. United States v. ChoicePoint, Inc. (Stipulated Final Judgment, FTC File No. 052 3069, N.D. Ga. Jan. 26, 2006), *available at* www.ftc.gov/os/caselist/choicepoint/choicepoint.htm

31. In the Matter of DSW Inc., (Agreement containing Consent Order, FTC File No. 052 3096, Dec. 1, 2005), *available at* www.ftc.gov/opa/2005/12/dsw.htm

32. In the Matter of BJ's Wholesale Club, Inc. (Agreement containing Consent Order, FTC File No. 042 3160, June 16, 2005), *available at* www.ftc.gov/opa/2005/06/bjswholesale.htm

33. In the Matter of Sunbelt Lending Services, Inc. (Agreement containing Consent Order, FTC File No. 042 3153, Nov. 16, 2004), *available at* www.ftc.gov/os/caselist/0423153/04231513.htm

34. In the Matter of Petco Animal Supplies, Inc. (Agreement containing Consent Order, FTC File No. 042 3153, Nov. 7, 2004), *available at* www.ftc.gov/os/caselist/0323221/0323221.htm

35. In the Matter of MTS, Inc., d/b/a Tower records/Books/Video (Agreement containing Consent Order, FTC File No. 032-3209, Apr. 21, 2004), *available* www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf

36. In the matter of Guess?, Inc. (Agreement containing Consent Order, FTC File No. 022 3260, June 18, 2003), *available at* www.ftc.gov/os/2003/06/guessagree.htm

37. FTC V. Microsoft (Consent Decree, Aug. 7, 2002), *available at* www.ftc.gov/os/caselist/0123240/0123240.shtm

38. In the Matter of Eli Lilly and Company (Decision and Order, FTC Docket No. C-4047, May 8, 2002), *available at* www.ftc.gov/os/2002/05/elililly do.htm

I. State Attorneys General Consent Decrees

1. In the Matter of Providence Health System-Oregon (Attorney General of Oregon, Assurance of Discontinuance), September 26, 2006, *available at* www.doj.state.or.us/releases/pdf/finfraud_providence_avc.pdf.

2. In the Matter of Barnes & Noble.com, LLC (Attorney General of New York, Assurance of Discontinuance, Apr. 20, 2004), *available at* www.bakerinfo.com/ecommerce/barnes-noble.pdf

3. In the Matter of Ziff Davis Media Inc. (Attorneys General of California, New York, and Vermont), Assurance of Discontinuance, Aug. 28, 2002), *available at* www.oag.state.ny.us/press/2002/aug/aug28a_02_attach.pdf

I. European Union – Directives

See http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

1. **EU Data Protection Directive**: European Union Directive 95/46/EC of February 20, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), Article 17, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

2. **EU Data Protection Directive:** European Union Directive 2006/24/EC of March 15, 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *available at* http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/745.pdf.

J. European Union – Security Provisions in Country Implementations of Data Protection Directive
See http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

1. **Belgium** –

   (a) Belgian Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, as modified by the law of 11 December 1998 Implementing Directive 95/46/EC, and the law of 26 February 2003; www.law.kuleuven.ac.be/icri/publications/499Consolidated_Belgian_Privacylaw_v200310.pdf. See Chapter IV, Article 16 (Confidentiality and security of processing**).**

   (b) See also, 13 February 2001 – Royal Decree Implementing the Act of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data.

2. **Czech Republic** – Consolidated version of the Personal Data Protection Act, Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/czech_republic_act_101_en.pdf See Articles 15, 27, 44, and 45.

3. **Cyprus** – Law of 2001, amended 2003; available at www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/138(I)-2001_en.pdf. See Article 10(3).

4. **Denmark** – Act on Processing of Personal Data,; *Act No. 429 of 31 May 2000,* (unofficial English translation); available at www.datatilsynet.dk/include/show.article.asp?art_id=443&sub_url=/lovgivning/indhold.asp&nodate=1. See Title IV, Part 11, Sections 41 and 42 (Security of processing).

5. **Estonia** -- Personal Data Protection Act; Passed 12 February 2003 (RT[1] I 2003, 26, 158), entered into force 1 October 2003; available at www.legaltext.ee/text/en/X70030.htm. See Chapter 3, Sections 18-20 (Personal Data Processing Requirements and Security Measures to Protect Personal Data).

6. **Finland** – The Finnish Personal Data Act (523/1999), given on 22.4.1999; available at www.tietosuoja.fi/uploads/hopxtvf.HTM. See Chapter 7, Sections 32-35 (Data security and storage of personal data**).**

7. **France** –ACT 78-17 of January 6th, 1978 on Data Processing, Data Files and Individual Liberties (Amended by the Act of 6 August 2004 Relating to the Protection of Individuals With Regard to the Processing of Personal Data, and by the Act of 12 May 2009 Relating to the Simplification and Clarification of Law and Lightening of Procedures); available at http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf. See Articles 34 and 35

8. **Germany** – **Germany** – Federal Data Protection Act (BDSG) In the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force from 1 September 2009; available at http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile. See Section 9 (Technical and organisational measures), Section 9a (Data protection audit), and Annex (to the first sentence of Section 9 of this Act).

9. **Greece** – Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended by Laws 2819/2000[126] and 2915/2001[127]); available at

[126] *Official Gazette 84 A 15.03.2000*

[127] *Official Gazette 109 A 19.05.2001*

www.dpa.gr/Documents/Eng/2472engl_all2.doc. See Article 10 (Confidentiality and security of processing).

10. **Hungary** – Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest; available at http://abiweb.obh.hu/dpc/index.php?menu=gyoker/relevant/national/1992_LXIII. See Article 10 (Data Security)**.**

11. **Ireland** – Data Protection Act of 1988; available at www.dataprivacy.ie/6ai.htm; Data Protection (Amendment) Act 2003; available at www.dataprivacy.ie/images/;Act2003.pdf. See Section 2.-(1), Security measures 2C, and First Schedule Article 7 (Data Security).

12. **Italy** – Personal Data Protection Code, Legislative Decree No. 196 of 30 June 2003; available at www.garanteprivacy.it/garante/document?ID=311066. See Chapter II (Minimum Security Measures) at Sections 33 (Minimum Security Measures), Section 34 (Processing by Electronic Means), Section 35 (Processing without Electronic Means), Section 36 (Upgrading), and Annex B (Technical Specifications Concerning Minimum Security Measures).

13. **Latvia** – Personal Data Protection Law, amended by Law of 24 October 2002; available at www.dvi.gov.lv/eng/legislation/pdp**.** See Section 26.

14. **Lithuania** – Law on Legal Protection of Personal Data, 21 January 2003, No. IX-1296, Official translation, with amendments 13 April 2004; available at www.ada.lt/images/cms/File/pers.data.prot.law.pdf. See Chapter 4, Article 24 (Security of Data).

15. **Luxembourg** – DPL approved on 2 August 2002 and published in Memorial A 91 of 13 August 2002. [*English version not available*].

16. **Malta** – Data Protection Act of December 14 2001 (Act XXVI of 2001), as amended by Act XXXI of 2002, Full entry into force July 15, 2003, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/malta_en.pdf. See Articles 26 and 27.

17. **Netherlands** – 25 892 - Rules for the protection of personal data (Personal Data Protection Act) (Unofficial translation); available at www.dutchdpa.nl/downloads_wetten/wbp.pdf. See Articles 13-15.

18. **Poland** –

    (a) Act of August 29, 1997 on the Protection of Personal Data, amended January 1, 2004, March 1, 2004, May 1, 2004; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/poland_en.pdf. See Articles 7, 31, 36, and 39a.

    (b) Ordinance of the Minister for Internal Affairs and Administration of 29 April 2004; documentation of processing of personal data and technical and organizational requirements which should be fulfilled by equipment and computer systems used for processing personal data (Journal of Laws of 1 May 2004).

19. **Portugal** – Act on the Protection of Personal Data (transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data); available at www.cnpd.pt/bin/legis/nacional/lei_6798en.htm. See Chapter II, Section III (Security and confidentiality of processing), at Article 14 (Security of processing), Article 15 (Special security measures), Article 16 (Processing by a processor), and Article 17 (Professional secrecy).

20. **Slovakia** – Act No 428 of 3 July 2002 on personal data protection; available at www.dataprotection.gov.sk/buxus/docs/act_no_428.pdf. See Chapter Two (Security of personal data), at Section 15 (Responsibility for personal data security), Section 16 (The security project), Section 17 (Instruction), Section 18 (Confidentiality obligation), and Section 19 (Personal data protection supervision).

21. **Slovenia** – Personal Data Protection Act, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/personal_data_protection_act_rs_2004.pdf. See Chapter 3, Articles 24 (Security of Personal Data), and Article 25 (Duty to Secure).

22. **Spain** –

    (a) Organic Law 15/1999 of 13 December on the Protection of Personal Data; available at https://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Ley_Organica_15-99_ingles.pdf. See Article 9 (Data security), Article 10 (Duty of secrecy).

    (b) Royal Decree 1720/2007, of 21 December, Which Approves The Regulation Implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data, unofficial translation available at https://www.agpd.es/portalweb/english_resources/common/reglamentolopd_en.pdf. See Articles 79 - 114 (Regarding security measures in the processing of personal data).

23. **Sweden** –

    (a) Personal Data Act (1998:204); issued 29 April 1998; available at www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf. See Security in processing at Section 30 (Persons who process personal data), Section 31 (Security measures), and Section 32 (The supervisory authority may decide on security measures).

    (b) Personal Data Ordinance (1998:1191); issued 3 September 1998, available at www.sweden.gov.se/content/1/c6/02/56/33/ed5aaf53.pdf.

24. **UK** – Data Protection Act 1998; available at www.hmso.gov.uk/acts/acts1998/19980029.htm. See Article 7 and The seventh principle.

K. Other Countries

1. **Argentina**: Act 25,326, Personal Data Protection Act (October 4, 2000), § 9; Security Measures for the Treatment and Maintenance of the Personal Data Contained in Files, Records, Databanks and Databases, either non state Public and Private (November 2006)

2. **Australia**: Privacy Act 1988, Act No. 119 of 1988 as amended taking into account amendments up to Act No. 86 of 2006, Schedule 3, Clause 4.

3. **Canada**: Personal Information Protection and Electronic Documents Act (2000, c. 5), Schedule 1, § 4.7.

4. **Hong Kong**: Personal Data (Privacy) Ordinance, December 1996, Schedule 1, Principle 4.

5. **Japan**: Act on the Protection of Personal Information, Law No.57, 2003, Articles 20, 21, 22, and 43

6. **South Korea**: The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., Amended by Act No. 7812, December 30, 2005, Articles 28, 29