# The New Law of Information Security: What Companies Need to Do Now 1

# Thomas J. Smedinghoff<sup>2</sup>

We are in the midst of a significant expansion of corporate obligations regarding security for digital information. Most businesses are, or soon will be, subject to two key legal obligations:

- A duty to provide reasonable security for their corporate data and information systems
- A duty to disclose security breaches to those who may be adversely affected by such breaches.

Although information security law has been developing for some time, pressures for enhanced corporate legal obligations to implement information security safeguards were accelerated by several recent highly publicized security breaches involving the loss or disclosure of sensitive personal information. Described by many as the "perfect storm," the controversy began with a February 15, 2005 disclosure by ChoicePoint, Inc., a company previously unknown to most people, that sensitive personal information it had collected on 145,000 individuals had been compromised, and was at risk of unauthorized use for purposes such as identity theft. In the five months that followed, over 60 additional companies, educational institutions, and federal and state government agencies, almost all household names, also disclosed breaches of the security of sensitive personal information in their possession, affecting a cumulative total of over 50 million individual records. And perhaps most significantly, the persons whose sensitive information was compromised included the chairman of the FTC and as many as 60 U.S. Senators

The reaction to these incidents has been a legislative and regulatory fury, at both the state and federal level. There has been a groundswell of support for the view that all corporate stakeholders have an interest in the security of corporate information, and that taking appropriate steps to ensure the security of that information, and to inform affected third parties of any breach, is a legal obligation for all companies. Thus, when the dust

<sup>&</sup>lt;sup>1</sup> Originally published in The Computer & Internet Lawyer Journal, November 2005, at pp. 9-25.

<sup>&</sup>lt;sup>2</sup> Thomas J. Smedinghoff, Baker & McKenzie, Chicago. Mr. Smedinghoff has been actively involved in developing e-business and information security legal policy both in the U.S. and globally. He currently serves as a member of the U.S. Delegation to the United Nations Commission on International Trade Law (UNCITRAL), where he participates in the Working Group on Electronic Commerce that recently completed negotiation of the *Convention on the Use of Electronic Communications in International Contracts*. He chaired the Illinois Commission on Electronic Commerce and Crime, and drafted the Illinois Electronic Commerce Security Act enacted in 1998. He served as an advisor to the National Conference of Commissioners on Uniform State Laws (NCCUSL) and participated in drafting the Uniform Electronic Transactions Act (UETA). He can be reached at *smedinghoff@bakernet.com*.

<sup>&</sup>lt;sup>3</sup> For a chronology of such breaches, and a running total of the number of individuals affected, see Privacy Rights Clearinghouse at <a href="https://www.privacyrights.org/ar/ChronDataBreaches.htm">www.privacyrights.org/ar/ChronDataBreaches.htm</a>.

settles, we are likely to see a more extensive codification of corporate legal obligations regarding the security of their own data, notwithstanding prior policy rejecting such a regulatory approach.<sup>4</sup>

It is important to recognize, however, that even without the additional legislation currently under consideration, almost all businesses today have some legal obligation to provide security for their own information. And satisfying that obligation is critical, especially in this highly-charged environment where a failure to do so is likely to bring on significant public relations problems as well as legal risk.

More importantly, a legal standard for compliance is emerging – i.e., a definition of "reasonable security." All of the major security-related statutes, regulations, and government enforcement actions of the past few years show an amazing consistency in approach. When viewed as a group, they set forth a rather clearly defined standard for legal compliance – one that requires a process-oriented approach to the development and maintenance of a comprehensive security program. Moreover, evidence suggests that even in cases not subject to such laws, this process-oriented approach is likely to be the standard against which legal compliance is measured.

As a result of recent security breaches, a legal corollary to the obligation to provide security has also received extensive legislative support. This is the duty to disclose security breaches to those who may be adversely affected by such breaches. That duty, which is focused primarily on personal information, is law in an ever-growing list of states, and will likely soon be federal law as well.

For both the duty to provide security and the duty to disclose breaches, this article will examine (1) the legal sources of the obligation, (2) the nature and scope of the duty, and (3) how companies should respond to address their compliance obligations. But first we take a look at where the law places the compliance responsibility.

### A. Responsibility for Corporate Information Security

Protecting the security of corporate information and computer systems was once just a technical issue to be addressed by the IT department. Today, however, as information security has evolved into a legal obligation, responsibility for compliance has been put directly on the shoulders of senior management, and in many cases the board of directors. It is, in many respects, a corporate governance issue.

Under the Sarbanes-Oxley Act, for example, responsibility lies with the CEO and the CFO.<sup>5</sup> In the financial industry, the Gramm-Leach-Bliley ("GLB") security regulations place responsibility for security directly with the Board of Directors.<sup>6</sup> In the

Sarbanes-Oxiey Act, Section 302

<sup>&</sup>lt;sup>4</sup> See, e.g., National Strategy to Secure Cyberspace, February 14, 2003, at p. 30, available at www.whitehouse.gov/pcipb.

<sup>&</sup>lt;sup>5</sup> Sarbanes-Oxley Act, Section 302.

<sup>&</sup>lt;sup>6</sup> See, e.g., GLB Security Regulations (Federal Reserve) 12 C.F.R. 208, Appendix D-2.III(A).

healthcare industry, the HIPAA security regulations require an identified security official to be responsibility for compliance. Several FTC consent decrees involving companies in a variety of non-regulated industries do likewise. And federal law places the responsibility for information security within each government agency on the head of such agency.

Evolving case law also suggests that, by virtue of their fiduciary obligations to the company, corporate directors will find that their duty of care includes responsibility for the security of the company's information systems. In particular, it may "extend from safeguarding corporate financial data accuracy to safeguarding the integrity of all stored data." In the *Caremark International Inc. Derivative Litigation*, for example, the Delaware court noted that "it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility." In the company of the co

The private sector is also beginning to recognize that the responsibility for security lies with upper management and the board of directors. The Business Roundtable, for example, has noted both that "[i]nformation security requires CEO attention" and that "[b]oards of directors should consider information security as an essential element of corporate governance and a top priority for board review." The Corporate Governance Task Force Report has taken a similar position, noting that:

The board of directors/trustees or similar governance entity should provide strategic oversight regarding information security, including:

- 1. Understanding the criticality of information and information security to the organization.
- 2. Reviewing investment in information security for alignment with the organization strategy and risk profile.
- 3. Endorsing the development and implementation of a comprehensive information security program.

10 E. Michael Power and Roland L. Trope, *Sailing in Dangerous Waters: A Director's Guide to Data Governance*, American Bar Association (2005), p. 13; Roland L. Trope, "Directors' Digital Fiduciary Duties," IEEE Security & Privacy, January/February 2005 at p. 78.

<sup>&</sup>lt;sup>7</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(2).

<sup>&</sup>lt;sup>8</sup> See, FTC Decisions and Consent Decrees listed in Appendix, including Microsoft Consent Decree at II, p. 4; Ziff Davis Assurance of Discontinuance, Para. 27(a), p. 7; Eli Lilly Decision at II.A.

<sup>&</sup>lt;sup>9</sup> FISMA, 44 U.S.C. 3544(a).

<sup>11</sup> Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).

<sup>&</sup>lt;sup>12</sup> Securing Cyberspace: Business Roundtable's Framework for the Future, Business Roundtable, May 19, 2004 at pp. 1, 2; available at <a href="www.businessroundtable.org/pdf//20040518000CyberSecurityPrinciples.pdf">www.businessroundtable.org/pdf//20040518000CyberSecurityPrinciples.pdf</a>. The Business Roundtable is an association of chief executive officers of leading U.S. corporations with a combined workforce of more than 10 million employees in the United States. See <a href="www.businessroundtable.org">www.businessroundtable.org</a>.

4. Requiring regular reports from management on the program's adequacy and effectiveness  $\frac{13}{2}$ 

The scope of that responsibility can also be significant. The GLB security regulations, for example, require the Board of Directors to approve the written security program, to oversee the development, implementation, and maintenance of the program, and to require regular reports (e.g., at least annually) regarding the overall status of the security program, the company's compliance with regulations, and material matters relating to the security program. 14

Similarly, under the Federal Information Security Management Act ("FISMA"), the head of each agency is responsible for providing information security protections, complying with the requirements of the statute, and ensuring that information security management processes are integrated within agency strategic and operational planning processes. The head of each agency is also required to appropriately delegate implementation tasks to the CIO and others. The HIPAA security regulations require that an identified security official be responsible for developing and implementing the required policies and procedures.

A key problem, however, is that the nature of the legal obligation to address security is often poorly understood by those levels in management charged with the responsibility, by the technical experts who must implement it, and by the lawyers who must ensure compliance. Yet, it is perhaps one of the most critical issues companies will face. As the recent series of highly-publicized security breaches has demonstrated, it is in many respects a time-bomb waiting to explode.

#### **B.** The Duty To Provide Security for Corporate Information

The legal issues surrounding information security are rooted in the fact that, in today's business environment, virtually all of a company's daily transactions, and all of its key records, are created, used, communicated, and stored in electronic form using networked computer technology. Electronic communications have become the preferred way of doing business, and electronic records have become the primary means for storing information. As a consequence, most business entities are now "fully dependent upon information technology and the information infrastructure." 15

<sup>13</sup> Information Security Governance: A Call to Action, Corporate Governance Task Force Report, National Cyber Security Partnership, April 2004, pp. 12-13, available at www.cyberpartnership.org/InfoSecGov4\_04.pdf. The National Cyber Security Partnership (NCSP) is led by the Business Software Alliance (BSA), the Information Technology Association of America (ITAA), TechNet and the U.S. Chamber of Commerce in voluntary partnership with academicians, CEOs, federal government agencies and industry experts. Following the release of the 2003 White House National Strategy to Secure Cyberspace and the National Cyber Security Summit, this public-private partnership was established to develop shared strategies and programs to better secure and enhance America's critical information infrastructure. Further information is available at www.cyberpartnership.org.

<sup>&</sup>lt;sup>14</sup> GLB Security Regulations (OCC), 12 C.F.R. Part 30, Appendix B, Part III.A and Part III.F.

<sup>15</sup> National Strategy to Secure Cyberspace, February 14, 2003, at p. 6, available at www.whitehouse.gov/pcipb.

This widespread implementation of networked information systems has provided companies with tremendous economic benefits, including significantly reduced costs and increased productivity. But the resulting dependence on a computer infrastructure also creates significant potential vulnerabilities that can result in major harm to the business and its stakeholders. Thus, concerns regarding corporate governance, ensuring individual privacy, protecting sensitive business data, accountability for financial information, and the authenticity and integrity of transaction data are driving the enactment of laws and regulations, both in the U.S. and globally, that are imposing obligations on businesses to implement information security measures to protect their own data.

# 1. <u>Security Generally</u>

The ultimate concern is electronic corporate information. But protecting electronic information also requires addressing the means by which such information is created, stored, and communicated. Thus, statutes and regulations governing information security typically focus on the protection of both *information systems* 17 – i.e., computer systems, networks, and software – as well as the *data, messages, and information* that is typically recorded on, processed by, communicated via, stored in, shared by, transmitted, or received from such information systems.

When addressing corporate information, it is also important to remember that all types of information need be considered, including financial information, personal information, tax-related records, employee information, transaction information, and trade secret and other confidential information. Moreover, the information can be in any form, including databases, e-mails, text documents, spreadsheets, voicemail messages, pictures, video, sound recordings, etc.

The objectives of information security are often stated in a variety of ways. In some cases, statutes and regulations define the primary objectives of information security in terms of positive results to be achieved, such as ensuring the *availability* of systems and information, controlling *access* to systems and information, and ensuring the

\_

<sup>&</sup>lt;sup>16</sup> "As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security." OECD Guidelines for the Security of Information Systems and Networks, July 25, 2002, at p. 7, available at www.oecd.org/dataoecd/16/22/15582260.pdf.

<sup>&</sup>lt;sup>17</sup> 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).

confidentiality, integrity, authenticity of information  $^{18}$  In other cases, they define the goals or objectives of security in terms of the harms to be avoided – e.g., to protect systems and information against unauthorized access, use, disclosure or transfer, modification or alteration, processing, and accidental loss or destruction.  $^{19}$ 

Regardless of approach, 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.

# 2. Where the Duty Comes From

Corporate legal obligations to implement security measures are set forth in an ever-expanding patchwork of federal and state laws, regulations, and government enforcement actions, as well as common law fiduciary duties and other implied obligations to provide "reasonable care." Many of the requirements are industry-specific (e.g., focused on the financial industry or the healthcare industry) or data-specific (e.g., focused on personal information or financial data). But in all cases they have been steadily expanding over the past several years, and that trend has been greatly accelerated by the series of high profile security breaches in early 2005.

Examples of some of the key sources of the duty to provide security that have been in place for several years include the following:

• Corporate governance legislation and caselaw designed to protect the company and its shareholders, investors, and business partners — Sarbanes-Oxley, for example, requires public companies to ensure that they have implemented appropriate information security controls with respect to their financial information. Similarly, several SEC regulations impose a variety of requirements for internal controls over information systems.

<sup>&</sup>lt;sup>18</sup> 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.

<sup>&</sup>lt;sup>19</sup> 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 Privacy Directive, Finland's Privacy Law, Italy's Privacy Law, and the UK Privacy Law. Also in this category is the Canadian Privacy Law.

<sup>&</sup>lt;sup>20</sup> A list of some of the key security laws and regulations is set out in the Appendix to this article. For a more comprehensive compilation of some of the laws and regulations governing information security, see <a href="https://www.bakernet.com/ecommerce">www.bakernet.com/ecommerce</a>.

<sup>&</sup>lt;sup>21</sup> See Sarbanes-Oxley Act, Sections 302 and 404. Sarbanes-Oxley is a good example of a statute that does not use the word "security," but that nonetheless requires significant security measures to ensure that adequate internal control structure and procedures for financial reporting are in place.

- Laws focused on the personal interests of individual employees, customers, or prospects Many privacy laws and regulations, particularly in the financial and healthcare sectors, require companies to implement information security measures to protect certain personal data they maintain about employees, customers, and prospects. <sup>22</sup>
- Laws addressing governmental regulatory interests or evidentiary 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. Many regulations do likewise. For example, IRS regulations require companies to implement information security to protect electronic tax records, and as a condition to engaging in certain electronic transactions, SEC regulations address security in a variety of contexts, and FDA regulations require security for certain records.
- Laws governing federal government agencies The comprehensive Federal Information Security Management Act of 2002 ("FISMA") addresses government security and requires security measures to protect all information collected or maintained by a federal agency, and all information systems used or operated by or for the agency. 28
- Common law In addition, several commentators have also argued that there
  may exist a common law duty to provide security, the breach of which
  constitutes a tort.<sup>29</sup>

<sup>&</sup>lt;sup>22</sup> See, e.g., Gramm-Leach-Bliley ("GLB") Act, Sections 501 and 505(b), 15 U.S.C. Sections 6801, 6805 and GLB Security 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); Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. 1320d-2 and 1320d-4, and HIPAA Security Regulations at 45 C.F.R. Part 164; and Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. 6501 *et seq.*, and COPPA regulations at 16 C.F.R. 312.8. See also, EU Data Protection Directive, Article 17, available at <a href="http://europa.eu.int/comm/internal\_market/privacy/docs/95-46-ce/dir1995-46">http://europa.eu.int/comm/internal\_market/privacy/docs/95-46-ce/dir1995-46</a> part1 en.pdf.

<sup>&</sup>lt;sup>23</sup> See Electronic Signatures in Global and National Commerce Act ("E-SIGN"), at 15 U.S.C. § 7001(d); Uniform Electronic Transaction Act ("UETA"), at § 12.

<sup>&</sup>lt;sup>24</sup> See, e.g., IRS Rev. Proc. 97–22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25.

<sup>25</sup> See, e.g., IRS Announcement 98-27, 1998-15 I.R.B. 30, and Tax Regs. 26 C.F.R. § 1.1441-1(e)(4)(iv).

<sup>&</sup>lt;sup>26</sup> See, e.g., 17 C.F.R. 240.17a-4, 17 C.F.R. 257.1(e)(3).

<sup>27</sup> See, e.g., 21 C.F.R. Part 11.

<sup>&</sup>lt;sup>28</sup> Federal Information Security Management Act of 2002 ("FISMA"), 44 U.S.C. Section 3544(a)(1)(A).

<sup>&</sup>lt;sup>29</sup> See, e.g., Margaret Jane Radin, Distributed Denial of Service Attacks: Who Pays? available at <a href="http://www.mazunetworks.com/white-papers/radin-print.html">http://www.mazunetworks.com/white-papers/radin-print.html</a>; Kimberly Kiefer and Randy V. Sabett, Openness of Internet Creates Potential for Corporate Information Security Liability, BNA Privacy & Security Law Report, Vol. 1, No. 25 at 788 (June 24, 2002); Alan Charles Raul, Frank R. Volpe, and Gabriel S. Meyer, Liability for Computer Glitches and Online Security Lapses, BNA Electronic Commerce Law Report, Vol. 6, No. 31 at 849 (August 8, 2001); Erin Kenneally, The Byte Stops Here: Duty and

While these statutes and regulations impose significant obligations on certain companies with respect to certain types of data, they are part of a growing trend to require all companies to provide appropriate security for all data, at least where the compromise of such data may damage the interests of corporate stakeholders. Several key developments support this expansion of coverage of security obligations.

Beginning in 2002, through a series of enforcement actions and consent decrees, both the FTC and several state attorneys general have pursued companies in a variety of industries bases on an alleged failure to provide adequate security for their data. However, the targeted companies were not directly subject to security regulation. Instead, these cases were based on the alleged failure of such companies to provide adequate information security contrary to representations to customers – i.e., claims of deceptive trade practices.  $\frac{30}{2}$ 

In early 2003, the Bush Administration released its *National Strategy to Secure Cyberspace*, which also argued for a much broader approach to corporate security obligations. Noting that most business entities "have become fully dependent upon information technology and the information infrastructure," the *National Strategy* sought to move the debate beyond specific industry sectors and specific types of data, asserting that "*all users* of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace." <sup>32</sup>

In March 2005 testimony before Congress, the Chairman of the Federal Trade Commission, Deborah Platt Majoras, provided further support for this view by suggesting that the extensive scope of the security obligations imposed on the banking industry should be expanded to cover all industries. And, in fact, this has essentially been FTC policy in its enforcement actions and resulting consent decrees since 2002. Moreover, in June 2005 the FTC broadened the scope of its enforcement actions by asserting that a failure to provide appropriate information security was, itself, an unfair trade practice

*Liability for Negligent Internet Security*, Computer Security Journal, Vol. XVI, No. 2, 2000, available at <a href="http://www.gocsi.com/pdfs/byte.pdf">http://www.gocsi.com/pdfs/byte.pdf</a>.

 $<sup>\</sup>frac{30}{2}$  See list of FTC Decisions and Consent Decrees and list of State Attorneys General Consent Decrees in the Appendix.

<sup>31</sup> National Strategy to Secure Cyberspace, February 14, 2003, at pp. 5-6, available at www.whitehouse.gov/pcipb

<sup>32</sup> National Strategy at page 37 (emphasis added).

<sup>&</sup>lt;sup>33</sup> See, Gramm-Leach-Bliley Act ("GLBA"), Public Law 106-102, Sections 501 and 505(b), 15 U.S.C. Sections 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).

<sup>&</sup>lt;sup>34</sup> "Senate Banking Committee Members Grill ChoicePoint Executive on Breaches," BNA Privacy & Security Law Report, March 21, 2005 at p. 351.

<sup>35</sup> See list of FTC Decisions and Consent Decrees in the Appendix.

under Section 5 of the FTC Act, even in the absence of any false representations by the defendant as to the state of its security.  $\frac{36}{}$ 

Recently filed lawsuits also suggest efforts to broaden the scope of corporate security obligations, with a view to protecting the interests of major stakeholders of all companies. Two class action lawsuits brought against ChoicePoint are good examples. The first suit, brought on behalf of individuals whose personal data was compromised by the security breach disclosed on February 15, 2005, alleges that ChoicePoint failed to implement adequate security measures, and failed to timely and fully disclose the breaches once they occurred. The second suit, brought on behalf of shareholders, alleges that ChoicePoint and its management failed to disclose to shareholders and potential investors that the company's security measures were inadequate and ineffective. The second suit, and the security measures were inadequate and ineffective.

At the same time, some states have begun passing laws imposing a general obligation to implement information security. 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. Other states have followed suit in 2005, including Arkansas, Nevada, and Rhode Island.

The bottom line is that a company's duty to provide security may come from several different sources, each perhaps asserting jurisdiction over a different aspect of corporate information. But the net result (and certainly the trend) is a general obligation to provide security for corporate data and information systems.

The nature and scope of that obligation, however, is not always clear. Often unanswered is a key question: Just what exactly is a business obligated to do? What is the scope of its legal obligations to implement information security measures?

<sup>36</sup> See, *In the Matter of BJ's Wholesale Club, Inc.* (Agreement containing Consent Order, FTC File No. 042 3160, June 16, 2005), available at <a href="https://www.ftc.gov/opa/2005/06/bjswholesale.htm">www.ftc.gov/opa/2005/06/bjswholesale.htm</a>.

<sup>37</sup> Goldberg v. ChoicePoint, Inc. No. BC329115, (Los Angeles Superior Ct., filed Feb. 18, 2005).

<sup>38</sup> Perry v. ChoicePoint, Inc. No. CV-05-1644 (C.D. Cal., filed March 4, 2005).

<sup>&</sup>lt;sup>39</sup> Cal. Civil Code Section 1798.81.5(b).

<sup>40</sup> Ark. Code Section 4-110-104(b).

<sup>41 52</sup> Nev. Rev. Stat. Section 23(1).

<sup>42</sup> R.I. Stat. 11-49.2-2(2) and (3).

# 3. The Legal Standard for Information Security

Laws and regulations rarely specify what specific security measures a business should implement to satisfy its legal obligations. Most simply obligate the company to establish and maintain internal security procedures, controls, safeguards, or measures directed toward achieving the goals or objectives identified above, but often without any further direction or guidance. The standard for compliance, if one is stated, often requires simply that the security be "reasonable" or "appropriate." Other expressions of the standard that appear in some regulations include "suitable," "necessary," and "adequate."

A critical problem, then, is assessing how far a company is "legally" obligated to go. When are the security measures it implements sufficient, *from a legal perspective*, to comply with its obligations? For, example, does installing a firewall and using virus detection software satisfy a company's legal obligations? Is it necessary for an organization to encrypt all of its electronic records? How does a business know when it is legally compliant? Is there a safe harbor? Since there is no such thing as perfect security (i.e., there is always more that you can do), <sup>47</sup> resolving these questions can significantly affect cost.

The FTC acknowledges that the mere fact that a breach of security occurs does not necessarily mean that there has been a violation of law. But it also notes that an organization can fail to meet its security obligations, even in the absence of a breach of that security. Thus, the key issue (from a legal perspective) is defining the scope and

<sup>&</sup>lt;sup>43</sup> Although they often focus on categories of security measures to address. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. Part 164.

<sup>44</sup> See, e.g., FDA regulations at 21 C.F.R. Part 11 (procedures and controls); SEC regulations at 17 C.F.R. 257.1(e)(3) (procedures); SEC regulations at 17 C.F.R. 240.17a-4 (controls); GLB regulations (FTC) 16 C.F.R. Part 314 (safeguards); Canada, Personal Information Protection and Electronic Documents Act, Schedule I, Section 4.7 (safeguards); EU Data Privacy Directive, Article 17(1) (measures) available at http://europa.eu.int/comm/internal\_market/privacy/docs/95-46-ce/dir1995-46\_part1\_en.pdf.

<sup>45</sup> See, e.g., HIPAA 42 U.S.C. 1302d-2, and HIPAA Security regulations, 45 CFR 164.306; COPPA, 15 U.S.C. 6502(b)(1)(D), and COPPA regulations 16 C.F.R. 312.8; IRS Rev. Proc. 97-22, sec. 4.01(2); SEC regulations 17 C.F.R. 257. See also UCC Article 4A, Section 202 ("commercially reasonable" security procedure), and Microsoft Consent Decree.

<sup>&</sup>lt;sup>46</sup> "Appropriate" security required by: HIPAA 42 U.S.C. 1302d-2, and HIPAA Security regulations, 45 CFR 164.306; EU Data Protection Directive, Article 17(1).

<sup>&</sup>lt;sup>47</sup> See, e.g., 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, available at <a href="https://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf">www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf</a> (noting that "the Commission recognized that there is no such thing as "perfect" security and that breaches can occur even when a company has taken all reasonable precautions"), at p. 4.

<sup>48</sup> *Id.* at p. 5, (noting that "'not all breaches of information security are violations of FTC law . . . . [B] reaches can happen, . . . even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces.").

<sup>&</sup>lt;sup>49</sup> Id. at p. 6, (noting that "there can be law violations without a known breach of security."). See also, Microsoft Consent Decree.

extent of a company's "legal" obligation to implement information security. In other words, what is the legal standard against which compliance with an obligation to provide reasonable security is measured?

There are many standards that seek to define the scope of information security requirements from a "technical" perspective. 50 But a review of newer statutes, regulations, and cases  $\frac{51}{2}$  indicates that a "legal" standard is also beginning to emerge – a legal standard that helps to clarify the scope and extent of a company's obligation to implement information security. Under that standard, which is described in detail below, the duty to provide information security (e.g., the duty to provide "reasonable" security) requires both (1) implementation of an ongoing process and (2) addressing certain categories of security measures.

The developing legal standard involves a relatively sophisticated approach to compliance, and recognizes what security consultants have been saying for some time: "security is a process, not a product." Thus, it does not literally dictate what security measures are required to achieve "reasonable security." Instead, it sets out requirements for a fact-specific process leading to the development of what is often referred to as a "comprehensive information security program," 53 and makes clear that following that process is required to achieve legal compliance.

This "process oriented" legal standard for corporate information security 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

<sup>50</sup> See, e.g., Jody Westby (Ed.), International Strategy for Cyberspace Security, at Chapter 4 (American Bar Association, Section of Science & Technology Law, 2004). Although none of these standards has yet become generally accepted in all industries, one that is commonly cited is ISO 17799, the "Code of Practices for Information Technology Management," adopted by the International Organization for Standardization (ISO) in August 2000 and revised in June 2005. (A copy of ISO 17799 is available at the ISO web site (www.iso.org) for a fee.) ISO 17799 is "becoming recognized practice for security management in private and public organizations." See Council of the European Union, Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security (2002/C 43/02), whereas clause number 11. The National Institute of Standards and Technology (NIST) has also developed an extensive set of standards. See http://csrc.nist.gov/publications/nistpubs/index.html.

 $<sup>\</sup>frac{51}{1}$  A list of some of the key statutes, regulations, and enforcement actions addressing corporate obligations to implement information security measures is set out in the Appendix.

<sup>&</sup>lt;sup>52</sup> Bruce Schneier, Secrets & Lies: Digital Security in a Networked World (John Wiley & Sons, 2000) at page XII. The FTC has also noted: "security is more a process than a state." See, Final Report of the FTC Advisory Committee on Online Access and Security, May 15, 2000, p.26, available at www.ftc.gov/acoas/papers/finalreport.htm

<sup>53</sup> See, e.g., FISMA, 44 U.S.C. Section 3544(b) ("develop, document, and implement an agencywide information security program"), GLB Regulations (Federal Reserve), 12 C.F.R. 208, Appendix D-2.II(A) ("Implement a comprehensive written information security program"); GLB Regulations (FTC), 16 C.F.R. 314.3(a) ("Develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts"); and Microsoft Consent Decree ("Establish and maintain a comprehensive information security program in writing").

the Office of Thrift Supervision, on February 1,  $2001,\frac{54}{}$  and later adopted by the FTC in its GLBA *Safeguards Rule* on May 23,  $2002.\frac{55}{}$  The same approach was also incorporated in the Federal Information Security Management Act of 2002 ("FISMA"), $\frac{56}{}$  and in the HIPAA *Security Standards* issued by the Department of Health and Human Services on February 20.  $2003.\frac{57}{}$ 

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. Thus, it has, in effect, implemented this "process oriented" approach in all of its decisions and consent decrees relating to alleged failures to provide appropriate information security. The National Association of Insurance Commissioners has also recommended the same approach, and to date, several state insurance regulators have adopted it. Several state Attorneys General have also adopted this approach in their actions against perceived offenders.

A careful review of the foregoing legislation, regulations, and consent decrees reveals an amazingly consistent approach that defines the parameters of the process-oriented legal standard for security. The overall theme is a recognition that determining appropriate security is a fact-specific exercise. Merely implementing seemingly strong security measures is not sufficient *per se*. Security measures must be responsive to existing threats facing the company, and must constantly evolve in light of changes in threats, technology, the company's business, and other factors.

<sup>&</sup>lt;sup>54</sup> 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).

<sup>55 67</sup> Fed. Reg. 36484, May 23, 2002; 16 C.F.R. Part 314.

<sup>56 44</sup> U.S.C. Section 3544(b).

<sup>57 45</sup> C.F.R. Parts 164.

<sup>58</sup> See, Final Report of the FTC Advisory Committee on Online Access and Security, May 15, 2000, p.26 (noting that "security is more a process than a state"), available at <a href="https://www.ftc.gov/acoas/papers/finalreport.htm">www.ftc.gov/acoas/papers/finalreport.htm</a>; and 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 <a href="https://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf">www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf</a>.

<sup>&</sup>lt;sup>59</sup> See, e.g., FTC Decisions and Consent Decrees listed in the Appendix.

<sup>60</sup> See, e.g., National Association of Insurance Commissioners "Standards for Safeguarding Customer Information Model Regulation" IV-673-1 available at <a href="https://www.naic.org">www.naic.org</a> (adopted in 9 states) See, e.g., State Attorneys General Consent Decrees listed in the Appendix

Thus, in most cases there are no hard and fast rules regarding which specific security measures to implement. Instead, the legal standard for security focuses on a process to identify and implement measures that are reasonable under the circumstances to achieve the desired security objectives. This requires companies to engage in an *ongoing and repetitive process* that is designed to assess risks, identify and implement responsive security measures, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.

#### 4. What Companies Need to Do

The essence of the process-oriented approach to security compliance is implementation of a comprehensive written security program that includes:

- Asset assessment identifying the systems and information that need to be protected
- Risk assessment conducting periodic assessments of the risks faced by the company
- Security measures developing and implementing security measures designed to manage and control the specific risks identified
- Address third parties overseeing third party service provider arrangements.
- Education implementing security awareness training and education
- Monitoring and testing to ensure that the program is properly implemented and effective
- Reviewing and adjusting to revise the program in light of ongoing changes.

The legally-mandated process may be summarized as follows:

#### (a) Asset Assessment

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) 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. This involves 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

<sup>62</sup> See, e.g., HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(A).

<sup>&</sup>lt;sup>63</sup> See, e.g., Microsoft Consent Decree at II, p. 4; Ziff Davis Assurance of Discontinuance, Para. 25(b), p. 5; Eli Lilly Decision at II.B; GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(1)

design, information processing, storage and disposal, prevention, detection, and response to attacks, intrusions, and other system failures, as well as employee training and management.  $\frac{64}{}$ 

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.<sup>65</sup>

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. 66

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.

# (c) <u>Develop Security Program to Manage and Control Risk</u>

Based on the results of the risk assessment, a business should 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 coordinated among all parts of the organization. It should be designed to provide reasonable safeguards to control the identified risks (i.e., to protect against any

<sup>65</sup> See, e.g., FISMA, 44 U.S.C. Sections 3544(a)(2)(A) and 3544(b)(1); GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(2)

<sup>&</sup>lt;sup>64</sup> See, e.g., Microsoft Consent Decree at II, p. 4; Eli Lilly Decision at II.B.

<sup>&</sup>lt;sup>66</sup> See, e.g., Authentication In An Electronic Banking Environment, July 30, 2001, Federal Financial Institutions Examination Council, page 2; available at www.occ.treas.gov/ftp/advisory/2001-8a.pdf.

<sup>&</sup>lt;sup>67</sup> See, e.g., Microsoft Consent Decree at II, p. 4; GLB Security Regulations (OCC), 12 C.F.R. Part 30 Appendix B, Part II.A; Eli Lilly Decision at II.B; HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(i); Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Section 3544(b).

<sup>&</sup>lt;sup>68</sup> See, e.g., Microsoft Consent Decree at II, p. 4; GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A; HIPAA Security Regulations, 45 C.F.R. Section 164.316(b)(1); Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Section 3544(b).

<sup>&</sup>lt;sup>69</sup> See, e.g., GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A; Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Section 3544(b).

<sup>&</sup>lt;sup>70</sup> See, e.g., Microsoft Consent Decree at II, p. 4; GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.B

anticipated threats or hazards to the security or integrity of the information and systems to be protected  $\frac{71}{2}$ ). The goal is to reduce the risks and vulnerabilities to a reasonable and appropriate level.  $\frac{72}{2}$ 

In other words, it is not enough merely to implement impressive-sounding security measures. They must be responsive to the particular threats a business faces, and must address its specific 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 and protect sensitive databases, but if a company's major vulnerability is careless (or malicious) employees who inadvertently (or intentionally) disclose passwords or protected information, then even those sophisticated technical security measures, while important, will not adequately address the problem.

#### (1) Relevant Factors to Consider

In determining what security measures should be implemented within a particular organization, virtually all of the 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. 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.  $\frac{74}{}$ 

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

<sup>&</sup>lt;sup>71</sup> See, e.g., GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.B(2); HIPAA Security Regulations, 45 C.F.R. Section 164.306(a)(2).

<sup>&</sup>lt;sup>72</sup> See, e.g., HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(B)

<sup>73</sup> See, e.g., United States v. Carroll Towing, 159 F.2d 169, 173 (2d Cir. 1947).

<sup>&</sup>lt;sup>74</sup> 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).

- 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  $\frac{75}{1}$

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, developing law in the U.S. 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 "may use any security measures" reasonably designed to achieve the objectives specified in the regulations. <sup>76</sup>

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. As one commentator has pointed out with respect to the HIPAA security regulations: "The new security rules offer no safe harbor to covered entities, business associates, or the people who make security decisions for them. Rather, whether security countermeasures are good enough to 'ensure' the confidentiality, integrity, and availability of [protected health information], and protect it from 'any' hazard one could reasonably anticipate, is likely to be judged retroactively." 77

Nonetheless, developing law seems to consistently require that companies consider certain *categories* of security measures, even if the way in which each category is addressed is not specified. At a high level, for example, most recent security rules require covered organizations to implement physical, technical, and administrative security measures.  $\frac{78}{2}$ 

<sup>77</sup> Richard D. Marks and Paul T. Smith, *Analysis and Comments on HHS's Just-released HIPAA Security Rules*, Bulletin of Law / Science & Technology, ABA Section of Science & Technology Law, No. 124 April 2003, at p. 2, available at http://www.abanet.org/scitech/DWTSecurityRules021703.pdf.

<sup>&</sup>lt;sup>75</sup> See, e.g., HIPAA Security Regulations, 45 C.F.R. Section 164.306(b)(2); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A and Part II.C; FISMA, 44 U.S.C. Sections 3544(a)(2) and 3544(b)(2)(B); Microsoft Consent Decree at II, p. 4; Ziff Davis Assurance of Discontinuance.

<sup>&</sup>lt;sup>76</sup> HIPAA Security Regulations, 45 CFR Section 164.306(b)(1).

<sup>78</sup> See, e.g., HIPAA regulations 45 C.F.R. Sections 164.308, 164.310, and 164.312; GLB Regulations, 12 C.F.R. 208, Appendix D-2.II(A) and 12 C.F.R. Part 30, Appendix B, Part II; Microsoft Consent Decree, at p. 4.

In addition, there are several more specific categories of security measures that regulations often require companies to consider. They include the following:

- Physical Facility and Device Security Controls procedures to safeguard the facility, <sup>79</sup> measures to protect against destruction, loss, or damage of information due to potential environmental hazards, such as fire and water damage or technological failures, <sup>80</sup> procedures that govern the receipt and removal of hardware and electronic media into and out of a facility, <sup>81</sup> and procedures that govern the use and security of physical workstations. <sup>82</sup>
- <u>Physical Access Controls</u> access restrictions at buildings, computer facilities, and records storage facilities to permit access only to authorized individuals <sup>83</sup>
- <u>Technical Access Controls</u> 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, <sup>84</sup> including procedures to determine access authorization, <sup>85</sup> procedures for granting and controlling access, <sup>86</sup> authentication procedures to verify that a person or entity seeking access is the one claimed, <sup>87</sup> and procedures for terminating access. <sup>88</sup>
- <u>Intrusion Detection Procedures</u> 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

<sup>&</sup>lt;sup>79</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.310(a)(2)(ii)

<sup>80</sup> GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.

<sup>81</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.310(d)

<sup>82</sup> HIPAA Security Regulations, 45 C.F.R. Sections 164.310(b) and (c)

<sup>83</sup> GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; HIPAA Security Regulations, 45 C.F.R. Section 164.310(a)

<sup>84</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(3)

<sup>85</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(3)(ii); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C

<sup>86</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(4) and 164.312(a); Ziff Davis Assurance of Discontinuance, Para. 25, p. 6

<sup>87</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.312(d)

<sup>88</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(3)(ii)(C)

<sup>89</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(5)(ii)(C)

- company information systems; <sup>90</sup> and procedures for preventing, detecting, and reporting malicious software (e.g., virus software, Trojan horses, etc.); <sup>91</sup>
- <u>Employee Procedures</u> job control procedures, segregation of duties, and background checks for employees with responsibility for or access to information to be protected, <sup>92</sup> and controls to prevent employees from providing information to unauthorized individuals who may seek to obtain this information through fraudulent means; <sup>93</sup>
- <u>System Modification Procedures</u> procedures designed to ensure that system modifications are consistent with the company's security program 94
- <u>Data Integrity, Confidentiality, and Storage</u> procedures to protect information from unauthorized access, alteration, disclosure, or destruction during storage or transmission, <sup>95</sup> including storage of data in a format that cannot be meaningfully interpreted if opened as a flat, plain-text file, <sup>96</sup> or in a location that is inaccessible to unauthorized persons and/or protected by a firewall; <sup>97</sup>
- <u>Data Destruction and Hardware and Media Disposal</u> procedures regarding final disposition of information and/or hardware on which it resides, <sup>98</sup>/<sub>98</sub> and procedures for removal from media before re-use of the media; <sup>99</sup>/<sub>99</sub>
- 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 101

<sup>&</sup>lt;sup>90</sup> GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Ziff Davis Assurance of Discontinuance, Para. 24(d), p. 5 and Para. 25, p. 6

<sup>91</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(5)(ii)(B)

<sup>92</sup> GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.

<sup>93</sup> GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.

<sup>&</sup>lt;sup>94</sup> GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Ziff Davis Assurance of Discontinuance, Para. 25, p. 6

<sup>95</sup> GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Ziff Davis Assurance of Discontinuance, Para. 25, p. 6; HIPAA Security Regulations, 45 C.F.R. Sections 164.312(c) and (e)

<sup>&</sup>lt;sup>96</sup> Ziff Davis Assurance of Discontinuance, Para. 25, p. 6

<sup>&</sup>lt;sup>97</sup> Ziff Davis Assurance of Discontinuance, Para. 25, p. 6

<sup>98</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.310(d)(2)(i)

<sup>&</sup>lt;sup>99</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.310(d)(2)(ii)

<sup>100</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.310(a)(2)(iv)

<sup>&</sup>lt;sup>101</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.312(b)

- <u>Contingency Plan</u> 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 102
- <u>Incident Response Plan</u> -- 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) 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. And 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. 104

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,  $\frac{105}{2}$  (2) they must contractually require outsource providers to implement appropriate security measures,  $\frac{106}{2}$  and (3) they must monitor the performance of the outsource providers.

<sup>102</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(7)

<sup>103</sup> Ziff Davis Assurance of Discontinuance, Paras. 24(d) and 26, pp. 5,6; HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(6)(i); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C

<sup>&</sup>lt;sup>104</sup> See, e.g., Office of the Comptroller of the Currency, Administrator of National Banks, OCC Bulletin 2001-47 on Third Party Relationships, November 21, 2001 (available at www.OCC.treas.gov/ftp/bulletin/2001-47.doc).

<sup>&</sup>lt;sup>105</sup> See, e.g., GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(1)

<sup>&</sup>lt;sup>106</sup> See, e.g., GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(2); HIPAA Security Regulations, 45 C.F.R. Section 164.308(b)(1) and 164.314(a)(2)

<sup>&</sup>lt;sup>107</sup> GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(3).

# (e) 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 U.S. 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.

### (f) 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, <sup>111</sup> and conducting regular testing or monitoring of the effectiveness of those measures. <sup>112</sup> Existing precedent also suggests that companies must monitor compliance with its security program. <sup>113</sup> To that end, a regular review of records of system activity, such as audit logs, access reports, and security incident tracking reports <sup>114</sup> is also important.

#### (g) 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

112 FISMA, 44 U.S.C. Section 3544(b)(5); Eli Lilly Decision at II.C; GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III(c)(3).

<sup>&</sup>lt;sup>108</sup> See, e.g., FISMA, 44 U.S.C. Section 3544(b)(4); HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(5)(i); Ziff Davis Assurance of Discontinuance, Para. 24(d), p. 5

<sup>109</sup> Ziff Davis Assurance of Discontinuance, Para. 27(c), p. 7.

<sup>110</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(C)

<sup>111</sup> Microsoft Consent Decree at II, p. 4

<sup>113</sup> Ziff Davis Assurance of Discontinuance, Para. 27(e) and (f), p. 7; Eli Lilly Decision at II.C.

<sup>&</sup>lt;sup>114</sup> HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(D)

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. 116

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.

# C. The Duty To Disclose Security Breaches

As a direct response to the large number of high-profile security breaches involving sensitive personal information, most states, and Congress, introduced legislation to require notification of persons affected by such breaches. Such laws and regulations focused not on imposing an obligation to *implement* security measures, but rather, on imposing an obligation to *disclose* security breaches. Thus, even where there is no duty to provide security, there may well be a duty to disclose a breach of security.

#### 1. Overview of the Duty

One of the first requirements to disclose breaches of security applied to taxrelated records, and appeared in 1998 regulations governing electronic records issued by the Internal Revenue Service. In a Revenue Procedure that sets forth the basic rules for maintaining tax-related records in electronic form, the IRS requires taxpayers to "promptly notify" the IRS District Director if any electronic records "are lost, stolen,

His Microsoft Consent Decree at II, p. 4; Ziff Davis Assurance of Discontinuance, Para. 27(e) and (f), p. 7; Eli Lilly Decision at II.D, GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.E; HIPAA Security Regulations, 45 C.F.R. Section 164.306(e) and 164.308(a)(8)

<sup>&</sup>lt;sup>116</sup> GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.E; HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(8); Microsoft Consent Decree at II, p. 4; Eli Lilly Decision at II.D

<sup>117</sup> Microsoft Consent Decree at III, p. 5

<sup>&</sup>lt;sup>118</sup> Ziff Davis Assurance of Discontinuance, Para. 27(h), p. 7

destroyed, damaged, or otherwise no longer capable of being processed ..., or are found to be incomplete or materially inaccurate."

Most recent legislation, however, has focused on the obligation to disclose breaches affecting sensitive personal information. Designed as a way to help protect persons who might be adversely affected by a security breach, these laws seek to impose 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 rules seek to provide such persons with an opportunity to take protective measures.

At the same time, these rules also leverage a very powerful force – the fact that the required disclosures may be embarrassing and serve to publicly highlight a company's lack of adequate security. Absent a legal requirement, most companies do not publicly disclose information security breaches or contact law enforcement agencies. The annual Computer Security Institute and FBI Computer Crime and Security Survey for 2005, <sup>120</sup> for example, reported that only 20 percent of respondents who suffered serious computer security breaches reported the incident to law enforcement. The key reason cited for not reporting intrusions to law enforcement, according to the Report, is the concern for negative publicity. Thus, the fear of adverse publicity arising from the obligation to disclose security breaches may actually incentivize companies to implement better security measures in the first place.

The first law requiring disclosure of security breaches involving personal information was the California Security Breach Information Act (S.B. 1386), which became effective on July 1, 2003. That law requires all companies doing business in California to disclose any breach of security that results in an unauthorized person acquiring certain types of personally identifiable information of a California resident. Disclosure must be made to all persons whose personal information was compromised, and anyone who is injured by a company's failure to do so can sue to recover damages. It is this law that is credited with requiring ChoicePoint (and all of the other companies that followed) to disclose the breaches they suffered in early 2005.

The ChoicePoint incident, and the other corporate breaches that followed, prompted many states to follow California's lead. Over 60 bills requiring notification of security breaches were quickly introduced in at least 36 states in Spring 2005. By August 2005, at least 20 states had enacted such laws, all essentially based on the California

-

<sup>119</sup> IRS Rev. Proc. 98-25, Section 8.01. The notice must identify the affected records and include a plan that describes how, and in what time frame, the taxpayer proposes to replace or restore the affected records in a way that assures that they will be capable of being processed. Rev. Proc. 98-25, Section 8.02.

<sup>120</sup> Available at www.gocsi.com

<sup>&</sup>lt;sup>121</sup> Cal. Civil Code Section 1798.82. A copy is available at www.leginfo.ca.gov/calaw.html.

model. Congress has followed suit with several bills of its own, all designed to impose security breach notification requirements on a nationwide basis. And several banking regulatory agencies have adopted regulations that also require notification of security breaches involving sensitive personal information. 122

# 2. 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:

- 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

<sup>122</sup> See, 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), adopted in March, 2005. These regulations require financial institutions to develop a response program to protect against and address breaches of the security of customer information maintained by the financial institution or its service provider. Such program must include procedures for notifying customers, as well as regulatory and law enforcement agencies, about incidents of unauthorized access to customer information that could result in substantial harm or inconvenience to the customer. The rules also require the financial institution to offer assistance to customers whose information was the subject of the incident (e.g., inform customers of their rights, recommend actions that they should take, assist them in the process, etc.).

- 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<sup>123</sup> 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 124 or unless the breach is material. 125

#### 3. **What Companies Need to Do**

How a company prepares for and responds to security breaches when they occur is a key issue. Prompt action on a variety of fronts is critical, both from a legal and a public relations perspective 126

The first step is planning. Given the proliferation of security breach notification laws, and the resulting duty to disclose breaches, there is a premium on taking steps, in advance, to reduce or eliminate the risk of having to make a disclosure. This begins with a review of information collection practices, both to identify where sensitive personal information is collected and stored, and to assess whether such information is really needed. In many cases, information subject to the security breach notification laws may not even be needed. But if it is, it is important that the company have an accurate understanding and inventory or what data it collects, and where it is stored. The bottom line is to identify notice-triggering information.

The next step, of course, is to ensure that appropriate security measures are in place to protect the personal information. To the extent that appropriate security can

<sup>123 15</sup> 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).

<sup>124</sup> Arkansas, Connecticut, Delaware, and Louisiana are examples of states in this category.

<sup>125</sup> Montana and Nevada are examples of states in this category.

<sup>126</sup> See generally, California Department of Consumer Affairs, Office of Privacy Protection, "Recommended Practices on Notification of Security Breach Involving Personal Information," October 10, 2003, available at www.privacy.ca.gov/recommendations/secbreach.pdf.

prevent breaches, and thus avoid the need for disclosure, it will be well worth the effort. This requires addressing the issues noted above in connection with the duty to provide security. Also worth noting is the fact that most security breach notification statutes apply only to the compromise of unencrypted personal information. Thus, to the extent reasonably feasible, encryption of all relevant personal information may well avoid the need to make any embarrassing disclosures.

It is also important to recognize that, as part of a comprehensive security program, companies need a well thought out and legally compliant incident response plan. In other words, how will it respond if a breach does occur? Such plan should ensure 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.

Such a plan should also clearly address how the company will comply with the requirements of the applicable security breach notification laws (which, unfortunately, do vary somewhat from state to state). This includes addressing issues such as whether a triggering event has occurred, how the affected individuals will be identified, the content, form and style of the notices, how notices will be communicated to the affected individuals, coordination with law enforcement (where relevant), and coordination with credit reporting agencies. It is also worth noting that some breach notification laws provide a safe harbor for companies that maintain internal data security policies that include breach notification provisions consistent with state law.

Finally, such planning needs to consider personal information in the control of third parties, such as outsource providers. Outsourcing information processing to a third party does not relieve a company of its obligations with respect to the security of the information outsourced, or its obligations to make disclosures in the event such information is the subject of a security breach. As a consequence, businesses will need to look carefully at the security measures of the outsource providers with whom they contract, and the measures in place, contractual and otherwise) to respond to breaches.

At some level, security breaches may be inevitable. But appropriate security can do a great deal to prevent them from occurring in the first place, and appropriate incident response planning can do a great deal to mitigate their effects and to limit both the legal damage and the reputation damage that would normally follow from such breaches.

# Appendix Key Information Security Law References

# A. <u>Statutes - Federal</u>

- 1. **COPPA**: Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. 6501 *et seq.*, available at <a href="https://www.ftc.gov/ogc/coppa1.htm">www.ftc.gov/ogc/coppa1.htm</a>
- 2. **E-SIGN**: Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001(d).
- 3. **FISMA**: Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Section 3541-3549, available at <a href="http://csrc.nist.gov/policies/FISMA-final.pdf">http://csrc.nist.gov/policies/FISMA-final.pdf</a>.
- 4. **GLA Act**: Gramm-Leach-Bliley Act, Public L. 106-102, Sections 501 and 505(b), 15 U.S.C. Sections 6801, 6805.
- 5. **HIPAA**: Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. 1320d-2 and 1320d-4.
- 6. **Homeland Security Act**: Homeland Security Act of 2002, 44 U.S.C. Section 3532(b)(1).
- 7. Sarbanes-Oxley Act: Sarbanes-Oxley Act, Pub. L. 107-204, Sections 302 and 404.

#### B. Statutes - State

1. **UETA**: Uniform Electronic Transaction Act, § 12 (now enacted in 46 states): www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

#### 2. Security Breach Notification Laws

- (a) Arkansas: <a href="https://www.arkleg.state.ar.us/ftproot/acts/2005/public/act1526.pdf">www.arkleg.state.ar.us/ftproot/acts/2005/public/act1526.pdf</a>.
- (b) California: <a href="http://info.sen.ca.gov/pub/01-02/bill/sen/sb\_1351-1400/sb\_1386">http://info.sen.ca.gov/pub/01-02/bill/sen/sb\_1351-1400/sb\_1386</a> bill 20020926 chaptered.html.
- (c) Connecticut: <u>www.cga.ct.gov/2005/act/Pa/2005PA-00148-R00SB-00650-PA.htm.</u>
- (d) Delaware: <a href="https://www.legis.state.de.us/LIS/lis143.nsf/vwLegislation/HB+116/\$file/legis.html?open">www.legis.state.de.us/LIS/lis143.nsf/vwLegislation/HB+116/\$file/legis.html?open</a>
- (e) Florida: <a href="https://www.myfloridahouse.gov/Sections/Documents/loaddoc.aspx?FileName=\_h048">www.myfloridahouse.gov/Sections/Documents/loaddoc.aspx?FileName=\_h048</a> 1er.doc&DocumentType=Bill&BillNumber=0481&Session=2005
- (f) Georgia: <a href="www.legis.state.ga.us/legis/2005\_06/fulltext/sb230.htm">www.legis.state.ga.us/legis/2005\_06/fulltext/sb230.htm</a>.
- (g) Illinois: www.ilga.gov/legislation/publicacts/fulltext.asp?Name=094-0036.
- (h) Indiana: www.in.gov/legislative/bills/2005/SE/SE0503.1.html.
- (i) Louisiana: www.legis.state.la.us/billdata/streamdocument.asp?did=320093.
- (j) Maine: <a href="http://janus.state.me.us/legis/LawMakerWeb/externalsiteframe.asp?ID=280017">http://janus.state.me.us/legis/LawMakerWeb/externalsiteframe.asp?ID=280017</a> 964&LD=1671&Type=1&SessionID=6.

- (k) Minnesota:
  - http://www.revisor.leg.state.mn.us/bin/bldbill.php?bill=H2121.3&session=ls84.
- (l) Montana: http://data.opi.state.mt.us/bills/2005/billhtml/HB0732.htm.
- (m) Nevada: www.leg.state.nv.us/73rd/bills/SB/SB347 EN.pdf.
- (n) New Jersey: www.bakerinfo.com/ecommerce/newjerseybreachlaw.pdf
- (o) New York: <a href="http://assembly.state.ny.us/leg/?bn=A04254&sh=t">http://assembly.state.ny.us/leg/?bn=A04254&sh=t</a>
- (p) North Dakota: www.state.nd.us/lr/assembly/59-2005/bill-text/FRBS0500.pdf.
- (q) Rhode Island:
  - www.rilin.state.ri.us/Billtext/BillText05/HouseText05/H6191.pdf.
- (r) Tennessee: www.legislature.state.tn.us/bills/currentga/BILL/SB2220.pdf.
- (s) Texas: <a href="www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&B">www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd
- (t) Washington: <a href="https://www.leg.wa.gov/pub/billinfo/2005-06/Htm/Bills/Session%20Law%202005/6043-S.SL.htm">www.leg.wa.gov/pub/billinfo/2005-06/Htm/Bills/Session%20Law%202005/6043-S.SL.htm</a>

# C. Regulations - Federal

- 1. **COPPA Regulations**: COPPA implementing regulations at 16 C.F.R. 312.8, available at www.ftc.gov/os/1999/10/64fr59888.htm.
- 2. FDA regulations at 21 C.F.R. Part 11, available at <a href="https://www.fda.gov/ora/compliance-ref/part11">www.fda.gov/ora/compliance-ref/part11</a>
- 3. 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 www.occ.treas.gov/consumer/Customernoticeguidance.pdf
- 4. **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), and 12 C.F.R. Part 568 (Office of Thrift Supervision), available at <a href="http://federalreserve.gov/boarddocs/press/boardacts/2001/20010117/attachment.pdf">http://federalreserve.gov/boarddocs/press/boardacts/2001/20010117/attachment.pdf</a>.
- 5. **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), available at <a href="https://www.ftc.gov/os/2002/05/67fr36585.pdf">www.ftc.gov/os/2002/05/67fr36585.pdf</a>
- 6. **HIPAA Security Regulations**: *Final HIPAA Security Regulations*, 45 C.F.R. Part 164, available at <a href="https://www.cms.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf">www.cms.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf</a>.
- 7. IRS Rev. Proc. 97–22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, available at <a href="https://www.intltaxlaw.com/INBOUND/reporting/rp9722.htm">www.intltaxlaw.com/INBOUND/reporting/rp9722.htm</a>, and Rev. Proc. 98-25, available at <a href="https://www.unclefed.com/Tax-Bulls/1998/rp98-25.pdf">www.unclefed.com/Tax-Bulls/1998/rp98-25.pdf</a>.

- 8. IRS Announcement 98-27, 1998-15 I.R.B. 30, and Tax Regs. 26 C.F.R. § 1.1441-1(e)(4)(iv).
- 9. SEC regulations at 17 C.F.R. 240.17a-4, and 17 C.F.R. 257.1(e)(3).

#### D. FTC Decisions and Consent Decrees

- 1. *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.
- 2. *In the Matter of Sunbelt Lending Services, Inc.* (Agreement containing Consent Order, FTC File No. 042 3153, November 16, 2004), available at <a href="https://www.ftc.gov/os/caselist/0423153/04231513.htm">www.ftc.gov/os/caselist/0423153/04231513.htm</a>.
- 3. *In the Matter of Petco Animal Supplies, Inc.* (Agreement containing Consent Order, FTC File No. 042 3153, November 7, 2004), available at <a href="https://www.ftc.gov/os/caselist/0323221/0323221.htm">www.ftc.gov/os/caselist/0323221/0323221.htm</a>.
- 4. *In the Matter of MTS, Inc., d/b/a Tower records/Books/Video* (Agreement containing Consent Order, FTC File No. 032-3209, April 21, 2004), available at www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf.
- 5. *In the matter of Guess?, Inc.* (Agreement containing Consent Order, FTC File No. 022 3260, June 18, 2003), available at <a href="https://www.ftc.gov/os/2003/06/guessagree.htm">www.ftc.gov/os/2003/06/guessagree.htm</a>.
- 6. FTC V. Microsoft (Consent Decree, August 7, 2002); available at <a href="https://www.ftc.gov/os/2002/08/microsoftagree.pdf">www.ftc.gov/os/2002/08/microsoftagree.pdf</a>
- 7. *In the Matter of Eli Lilly and Company*, (Decision and Order, FTC Docket No. C-4047, May 8, 2002); available at <a href="www.ftc.gov/os/2002/05/elilillydo.htm">www.ftc.gov/os/2002/05/elilillydo.htm</a>

#### E. State Attorneys General Consent Decrees

- 1. *In the Matter of Barnes & Noble.com, LLC* (Attorney General of New York, Assurance of Discontinuance, April 20, 2004); available at <a href="https://www.bakerinfo.com/ecommerce/barnes-noble.pdf">www.bakerinfo.com/ecommerce/barnes-noble.pdf</a>.
- 2. *In the Matter of Ziff Davis Media Inc.* (Attorneys General of California, New York, and Vermont), Assurance of Discontinuance, August 28, 2002); available at <a href="https://www.oag.state.ny.us/press/2002/aug/aug28a\_02\_attach.pdf">www.oag.state.ny.us/press/2002/aug/aug28a\_02\_attach.pdf</a>

#### F. European Union

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 <a href="http://europa.eu.int/comm/internal\_market/privacy/docs/95-46-ce/dir1995-46">http://europa.eu.int/comm/internal\_market/privacy/docs/95-46-ce/dir1995-46</a> part1 en.pdf.

# G. Other

- 1. *National Strategy to Secure Cyberspace*, February 14, 2003, available at <a href="https://www.whitehouse.gov/pcipb">www.whitehouse.gov/pcipb</a>
- 2. *Information Security Law Resources* (compilation of laws governing cybersecurity), available at <a href="https://www.bmck.com/ecommerce/home-security.htm">www.bmck.com/ecommerce/home-security.htm</a>