CHAPTER 14

INFORMATION SECURITY

§ 14.01 IN GENERAL

Over the last decade, advances in communication and computer technologies have revolutionized the way information is collected, used, and stored. The ease with which huge volumes of personal information are transmitted across the globe has changed the legal and policy landscape with respect to privacy and information security issues. In the information security arena, the legal regime has evolved from a largely unregulated environment to a highly complex scheme of federal and state law. Adding to the mélange of laws are significant and highly influential industry standards. At their most basic level, information security laws and standards are designed to protect against unauthorized access to and use, destruction, modification, or disclosure of personal information. There is no omnibus information security law in the United States that impacts all organizations in the same manner. U.S. businesses face a patchwork of information security mandates, including sector-specific federal laws and state laws that impose de facto national standards.

§ 14.02 APPLICABLE LAW

[A] Gramm-Leach-Bliley Act

[1] Overview

The Gramm-Leach-Bliley Act (GLB)[1] was enacted in 1999 to "enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies and other financial service providers. . . ."[2] GLB removed the legal barriers to affiliation among various types of financial institutions created by the Glass-Steagall Act of 1933,[3] allowing for the creation of diversified financial services holding companies. Congress also included in the law important privacy and information security provisions governing the use and disclosure by financial institutions of "nonpublic personal

[1] 15 U.S.C.A. §§ 6801–6809 (West 2007).

[2] H.R. Rep. No. 106-434, at 245 (1999) (Conf. Rep.).

[3] 12 U.S.C.A. § 24 (West 2007). The Glass-Steagall Act was enacted in response to the Great Depression. It restricted the ability of different types of financial institutions, such as banks, insurers, and investment banks, from affiliating with one another to form large financial services holding companies.

information'' (NPI) about their customers and consumers.[4] Specifically, Title V of GLB sets forth certain restrictions on disclosures of NPI, provides exceptions to these restrictions, and requires various federal functional regulators to adopt appropriate regulations to ensure the security and confidentiality of NPI. GLB's privacy requirements apply to all financial institutions, while the federal functional regulators' rules apply to entities subject to their jurisdiction.

When Congress enacted GLB, it required eight federal functional regulators and each state's insurance regulator to issue regulations pursuant to the law.[5] At the federal level, the relevant regulators include the federal banking agencies, the National Credit Union Administration (NCUA), the Secretary of the Treasury, the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC). Insurance providers that constitute ''financial institutions'' for GLB purposes are subject to the relevant state statutes and regulations promulgated by state insurance regulators. The regulatory schemes implemented by the various federal agencies and state regulators pursuant to GLB are substantially similar. Given its jurisdictional reach, the FTC's regulations implementing GLB impact the broadest range of financial institutions. The relevant regulations promulgated by the FTC are known as the Privacy Rule[6] and Safeguards Rule.[7] Information security is addressed by the Safeguards Rule. The FTC's requirements are discussed below.

[2] Definitions

The FTC Privacy Rule and Safeguards Rule apply to NPI. NPI means ''personally identifiable financial information'' that is (1) provided by a consumer to a financial institution, (2) about a consumer resulting from a transaction or service performed for the consumer, or (3) otherwise obtained by the financial institution.[8] *Personally identifiable financial information* includes any information obtained by a financial institution in connection with its provision of a ''financial product or service,'' even if the information is not typically considered financial in nature.[9] This

[4] 15 U.S.C.A. § 6801 (West 2007).
[5] *Id.*
[6] 16 C.F.R. pt. 313 (2008).
[7] 16 C.F.R. pt. 314.
[8] 16 C.F.R. § 313.3.
[9] 16 C.F.R. § 313.3(o).

definition is extremely broad and includes such information as the fact that an individual is a customer of a given financial institution.[10] Excluded from the definition of NPI are: (1) information that the financial institution has a "reasonable basis" to believe is publicly available and (2) any consumer list that is derived without using personally identifiable financial information.[11] An example of information that would not be considered NPI is certain mortgage information in a jurisdiction where such information is publicly recorded.[12]

[3] Safeguards Rule

GLB requires financial institutions to ensure the security and confidentiality of NPI.[13] The FTC's Safeguards Rule states that financial institutions must implement reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of NPI.[14] To do so, financial institutions must develop a written information security program.[15] The information security program should be tailored to a financial institution's (1) size and complexity, (2) nature and scope of its activities, and (3) sensitivity of the NPI it maintains.[16] The Safeguards Rule requires that the information security program include the following objectives: to (1) insure the security and confidentiality of NPI, (ii) protect against any anticipated threats or hazards to the security or integrity of NPI, and (iii) protect against unauthorized access to or use of NPI that could result in substantial harm or inconvenience to any customer.[17]

A financial institution subject to the Safeguards Rule must designate one or more employees to coordinate the information security program.[18] In addition, internal and external risks to the security, confidentiality, and integrity of NPI that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of NPI must be identified and

---

[10] Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646, 33,658 (May 24, 2000) (codified at 16 C.F.R. pt. 313).

[11] 16 C.F.R. § 313.3(o)(2)(ii) (2008).

[12] 16 C.F.R. § 313.3(p)(3)(iii)(A).

[13] 15 U.S.C.A. § 6801(b)(2) (West Supp. 2009).

[14] 16 C.F.R. § 314.3 (2008).

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

assessed in every area of operation.[19] Based on the risk assessment, the financial institution must evaluate the current safeguards in place to control identified risks.[20] The Safeguards Rule requires that the covered entity regularly monitor and test the information security program to determine its effectiveness.[21] Where weaknesses are identified, or changes occur in the business's operations, the information security program must be adjusted to address such issues.[22]

The information security program also must address a financial institution's retention of service providers that have access to NPI.[23] The Safeguards Rule indicates that covered entities may retain only those service providers that can maintain appropriate safeguards.[24] The covered entity must have a contract with the service provider, and the contract is required to stipulate appropriate safeguards with respect to the handling of NPI.[25]

The Safeguards Rule allows for some flexibility in the structure of the information security program, allowing financial institutions to implement safeguards that are appropriate to their operations.[26] To illustrate the flexible nature of the information security program requirement, the FTC notes that some institutions may choose to establish their information security program in a single document, whereas others may adopt several different policies and procedures to achieve a similar goal.[27] In addition, certain institutions may select one individual to be responsible for coordinating the information security program, while others may designate several such individuals.[28]

The Safeguards Rule also requires financial institutions to address risks to NPI, specifically focusing on three areas critical to promoting information security: (1) employee management and training, (2) information systems, and (3) detecting and managing system failures.[29]

---

[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] 16 C.F.R. § 314.3.
[27] FTC, Facts for Business: Financial Institutions and Customer Information: Complying with the Safeguards Rule (Apr. 2006), http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus54.shtm (last visited Aug. 17, 2009) [hereinafter Facts for Business].
[28] 16 C.F.R. § 314.4 (2008).
[29] *Id.*

[4] Federal Trade Commission Recommendations

The FTC has indicated that the success of any information security program hinges on those employees responsible for its implementation.[30] The FTC has provided recommendations regarding employees' roles with respect to the protection of NPI, suggesting that financial institutions consider:

1. verifying references and conducting background checks prior to hiring employees who will, as part of their role, have access to NPI;
2. requesting that new employees sign a contractual agreement to abide by the information security program;
3. limiting access to NPI exclusively on a need-to-know basis;
4. limiting access to NPI through the use of strong passwords that must be frequently altered;
5. developing policies and procedures to help ensure the appropriate use and protection of laptops, PDAs, and other mobile devices;
6. training employees to take steps to maintain the security, confidentiality, and integrity of NPI;
7. providing regular reminders of existing policies and procedures and legal requirements to keep NPI secure and confidential; and
8. imposing disciplinary measures for violations of the information security program.[31]

The Safeguards Rule requires financial institutions to identify and control risks within information systems, including network and software design, as well as information processing, storage, transmission, and disposal.[32] This involves maintaining security throughout the life cycle of the data, beginning with collection and ending with secure disposal. The FTC recommends that financial institutions know where NPI is stored and

[30] FTC, Facts for Business, *supra* note 27.
[31] *Id.*
[32] 16 C.F.R. § 314.4 (2008).

ensure that such storage is secure. Additionally, only authorized employees should have access to NPI. Specific FTC recommendations include:

1. verifying that NPI storage areas are protected against destruction or damage from hazards such as natural disasters;
2. storing institutional records in a physical location that is locked;
3. ensuring that strong passwords are maintained to access electronic records;
4. maintaining secure backup records and securing archived data appropriately;
5. maintaining a careful inventory of computers and other equipment containing NPI; and
6. securely transmitting NPI by adopting encryption standards or secure socket layer technology.[33]

Once NPI is no longer needed for business or legal reasons, the Safeguards Rule requires that covered entities dispose of the information securely.[34] To do so, the FTC recommends that financial institutions consider designating or retaining an individual responsible for records management and secure records disposal.[35] When disposing of records containing NPI, covered entities should consider burning, pulverizing, or shredding papers so that the information cannot be read or reconstructed. This recommendation is consistent with state laws and rules promulgated by the FTC outside the context of GLB.[36]

Compliance with the Safeguards Rule requires financial institutions to detect, prevent, and respond to attacks, intrusions, or other systems failures. On a practical level, this involves implementing reasonable measures to prevent attacks, identifying security incidents, and adopting a response plan should such events occur. To comply with the Safeguards Rule, financial institutions should consider learning about nascent threats and available protections. In addition, appropriate procedures should be adopted to keep logs of network activity and monitor in- and outbound data

---

[33] FTC, Facts for Business, *supra* note 27.

[34] 16 C.F.R. § 314.4 (2008).

[35] FTC, Facts for Business, *supra* note 27.

[36] *See, e.g.*, Cal. Civ. Code § 1798.81 (West, Westlaw 2010); Ga. Code Ann. § 10-15-2 (LEXIS 2009); Wash. Rev. Code Ann. § 19.215.020(1) (West, Westlaw 2009); Wis. Stat. Ann. § 134.97 (West, Westlaw 2009).

transfers. When there is an unauthorized intrusion into systems, covered entities must take immediate action to secure the information that may have been compromised. The Safeguards Rule also imposes an obligation of ongoing compliance with relevant information security requirements. Covered entities should continuously evaluate their information security program and, where necessary, update the program to reflect any material changes to business operations or any other relevant circumstances affecting the program's effectiveness.

[B] Health Insurance Portability and Accountability Act of 1996[37]

[1] Overview

Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[38] to help ensure the privacy and security of certain health information. In passing HIPAA, Congress called on the Department of Health and Human Services (HHS) to promulgate regulations that would further this objective. These regulations, known as the Privacy Rule[39] and the Security Rule,[40] apply to "covered entities" and limit the ability of such entities to use and disclose "protected health information" (PHI). HIPAA defines *covered entity* as a health plan, health care clearinghouse, or health care provider who transmits health information in electronic form in connection with certain specified transactions. *Protected health information* is defined as "individually identifiable health information . . . that is: (i) [t]ransmitted by electronic media; (ii) [m]aintained in electronic media; or (iii) [t]ransmitted or maintained in any other form or medium."[41]

---

[37] For more information, see Chapter 4.

[38] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.).

[39] 45 C.F.R. pt. 160 and §§ 164.102–164.106, 164.500–164.534 (2008).

[40] 45 C.F.R. pts. 160, 162, 164.

[41] 45 C.F.R. § 160.103. The definition excludes "individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer." *Id. Individually identifiable health information* means

> information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by

While the Privacy Rule contains broad data security requirements, the responsibility of a covered entity to secure electronic PHI is addressed principally (and specifically) by the Security Rule.

[2] Privacy Rule

HIPAA's Privacy Rule contains a broad security requirement that obligates every covered entity to protect the PHI it maintains.[42] Specifically, covered entities are required to implement:

> administrative, technical and physical safeguards to protect the privacy of protected health information. . . . A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of [the Privacy Rule] . . . [and] must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.[43]

It is important to note that the security requirement in the Privacy Rule applies to PHI in any format, whereas the Security Rule applies only to *electronic* PHI.

[3] Security Rule

The Security Rule imposes an obligation on every covered entity to ensure the confidentiality, integrity, and availability of all electronic PHI[44] the covered entity creates, receives, maintains, or transmits.[45] Pursuant to the Security Rule, a covered entity is required to (1) conduct a risk

---

> a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Id.

[42] 45 C.F.R. § 164.530(c).

[43] *Id.*

[44] *Id.*

[45] 45 C.F.R. § 164.306 (2008).

assessment of the potential risks and vulnerabilities to the confidentiality of electronic PHI held by the covered entity and (2) implement a risk management program to reduce the identified risks and vulnerabilities to a reasonable and appropriate level.[46] Covered entities must have in place certain specified administrative, physical, and technical safeguards to protect the electronic PHI they maintain.[47]

Administrative safeguards are:

> administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.[48]

Examples of administrative safeguards are (1) conducting risk assessments to determine the vulnerability of electronic PHI and implementing appropriate security measures to address any identified vulnerabilities, (2) conducting security awareness and training programs, and (3) conducting periodic evaluations of security policies and procedures.[49]

Physical safeguards are:

> physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.[50]

Physical safeguards include (1) facility access controls such as electronic badge systems and visitor logs; (2) workstation security controls; and (3) device and media controls, including procedures for data backup, storage, and final disposition of electronic PHI.[51]

Technical safeguards are "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."[52] Technical safeguards include (1) role-based access controls based on unique usernames and passwords, (2) audit controls to

---

[46] 45 C.F.R. § 164.308.
[47] 45 C.F.R. §§ 164.308, 164.310, 164.312.
[48] 45 C.F.R. § 164.304.
[49] 45 C.F.R. § 164.308.
[50] 45 C.F.R. § 164.304.
[51] 45 C.F.R. § 164.310.
[52] 45 C.F.R. § 164.304.

monitor activity in IT systems, and (3) transmission security such as encryption of data transfers.[53]

The Security Rule also requires covered entities to execute "business associate agreements" with any organization performing or assisting the covered entity with an activity that involves the use or disclosure of electronic PHI.[54]

[4] HITECH Act

The American Recovery and Reinvestment Act of 2009[55] (ARRA) was enacted in response to an economic downturn in the United States. The majority of ARRA's provisions focused on economic stimulus, including the Health Information Technology for Economic and Clinical Health Act[56] (HITECH Act), which was intended to promote increased reliance on electronic health records and generate a corresponding reduction in costs and inefficiencies associated with heavy reliance on hard-copy records. Certain provisions of the HITECH Act were intended, however, not to stimulate the economy but rather to improve the security of electronic health records. These provisions: (1) substantially broadened HIPAA's Security Rule and (2) established new information security breach notification requirements that apply to a wide range of businesses.

The HITECH Act broadened the scope of the Security Rule by imposing new legal obligations on business associates of covered entities.[57] Previously, business associates were merely contractually bound to comply with any security provisions included in their business associates agreements, which provisions were generally less onerous than the Security Rule's requirements for covered entities. In enacting the HITECH Act, Congress imposed the obligations of HIPAA's Security Rule directly on business associates.[58] The result is that business associates must now comply with each of the Security Rule's provisions that mandate specific administrative, physical, and technical safeguards, including the Rule's policies, procedures, and documentation requirements.

---

[53] 45 C.F.R. § 164.312. Additional safeguards are discussed in Chapter 4.

[54] 45 C.F.R. § 164.314.

[55] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 115 (2009).

[56] ARRA §§ 13001–13424, 4001–4302.

[57] ARRA, 123 Stat. 260.

[58] *Id.*

As directed by the HITECH Act, the Secretary of HHS, in August 2009, issued an interim final rule addressing the HITECH Act's security breach notification requirements, which apply with respect to unsecured PHI.[59] Pursuant to the HITECH Act, *unsecured PHI* means "protected health information that is not secured through the use of a technology or methodology specified by the Secretary. . . ."[60] HHS issued guidance in April 2009 pursuant to this provision in the HITECH Act whereby it declared that PHI is considered unsecured unless it has been encrypted in accordance with the HIPAA Security Rule or the media on which the PHI is stored has been securely shredded or destroyed.[61] Specifically, the HHS guidance endorses encryption processes for (1) data at rest that are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices; and (2) data in motion that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2.[62] For secure disposal, the HHS requires shredding or destruction of (1) paper, film, or other hard-copy media such that the PHI cannot be read or otherwise reconstructed, and (ii) electronic media by clearing, purging, or destroying consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.[63]

The HHS Interim Final Rule applies to all breaches of unsecured PHI discovered by covered entities and business associates.[64] A "breach" is defined as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such

---

[59] Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (to be codified at 45 C.F.R. pts. 160 and 164) [hereinafter HHS Interim Final Rule].

[60] ARRA § 13402(h)(1)(A).

[61] Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable for Purposes of the HITECH Breach Notification Requirements, 74 Fed. Reg. 19,006, 19,009–19,010 (Apr. 27, 2009) (to be codified at 45 C.F.R. pts. 160 and 164).

[62] *Id.*; *see also* National Inst. of Standards & Tech., Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices (2007); National Inst. of Standards & Tech., Federal Information Processing Standards 140-2, Security Requirements for Cryptographic Modules (2001).

[63] Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable for Purposes of the HITECH Breach Notification Requirements, 74 Fed. Reg. at 19,010; *see also* National Inst. of Standards & Tech., Special Publication 800-88, Guidelines for Media Sanitization (2006).

[64] Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. at 42,740, 42,744.

information is disclosed would not reasonably have been able to retain such information."[65] With respect to such breaches, the HHS Interim Final Rule requires covered entities to (1) notify individuals if their protected health information is subject to a security breach, (2) notify the Secretary of HHS, and (3) notify prominent media outlets in the event of a breach that affects 500 or more individuals.[66] Business associates experiencing a breach are required to notify the affected HIPAA-covered entity.[67] The HITECH Act also requires personal health record vendors and other non-HIPAA-covered entities to notify both affected individuals and the FTC following discovery of any breach of unsecured personal health records.[68] *Personal health record* is defined as "an electronic record of PHR identifiable health information[69] . . . on an individual that can be drawn from

---

[65] ARRA, Pub. L. No. 111-5, § 13400(1), 123 Stat. 115 (2009). The term does not include the following:

> (i) any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if—(I) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and (II) such information is not further acquired, accessed, used, or disclosed by any person; or
>
> (ii) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and
>
> (iii) any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

Id.

[66] Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. at 42,740, 42,752.

[67] ARRA, Pub. L. No. 111-5, § 13402, 123 Stat. 115 (2009); *see also* Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. at 42,740.

[68] ARRA § 13407; *see also* Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. at 42,741.

[69] The term *PHR identifiable health information* means:

> [I]ndividually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and includes, with respect to an individual, information—(A) that is provided by or on behalf of the individual; and (B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

ARRA § 13,407(f)(2).

multiple sources and that is managed, shared, and controlled by or primarily for the individual.''[70] The FTC in turn is required to notify the Secretary of HHS.[71] In this context, violations of the notice provisions are treated as unfair or deceptive acts, and the FTC is authorized to enforce these provisions under section 5 of the Federal Trade Commission Act.[72]

In August 2009, the FTC issued a final rule pursuant to the HITECH Act addressing security breaches of personal health records.[73] The FTC Final Rule applies to all foreign and domestic vendors of personal health records, personal health record–related entities, and third-party service providers that maintain information regarding U.S. citizens or residents.[74] The FTC Final Rule does not apply to HIPAA-covered entities or business associates.[75]

[C] Federal Information Security Management Act

[1] Overview

The Federal Information Security Management Act (FISMA)[76] requires federal agencies (which FISMA defines to include government and government-controlled corporations) to develop, document, and implement an agency-wide program to provide information security for (1) information collected or maintained by or on behalf of the agency and (2) ''information systems'' that support the operations and assets of the agency and are used or operated by the agency or its contractor or other organization on behalf of the agency.[77]

''Information'' subject to FISMA is broadly defined. Implementing regulations define *information* to include ''any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or

---

[70] ARRA § 13400(11).

[71] ARRA § 13407(d).

[72] ARRA § 13407(e).

[73] Health Breach Notification Rule, 74 Fed. Reg. 42,962 (Aug. 25, 2009) (to be codified at 16 C.F.R. pt. 318) [hereinafter FTC Final Rule].

[74] 74 Fed. Reg. at 42,980 (to be codified at 16 C.F.R. § 318.1).

[75] *Id.*

[76] Pub. L. No. 107-347, 116 Stat. 2899 (2002) (codified in scattered sections of 44 U.S.C.).

[77] 44 U.S.C.A. § 3543(a)(2) (West 2007).

audiovisual forms."[78] This definition also encompasses *information in identifiable form*, which is defined as:

> information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.[79]

Information systems within the scope of FISMA also are broadly defined to include any "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information."[80]

FISMA does not contain specific information security requirements that agencies must implement. Instead, the statute sets forth the process that agencies must follow in developing risk-based information security programs. FISMA requirements are implemented by the NIST regulations, including the Federal Information Processing Standards (FIPS) and Special Publications (SP). NIST standards and publications set out in detail the steps of the compliance process and the specific information security requirements agencies must implement based on the risk associated with relevant information and information systems. To be effective, an information security program required by FISMA should include the following elements:

- "[p]eriodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of [relevant] information and information systems";[81]

---

[78] *See* Office of Mgmt. & Budget, OMB Circular No. A-130, Management of Federal Information Resources (2000).

[79] Office of Mgmt. & Budget, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (2003) ("These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors."). More generally, *personally identifiable information* means information in "identifiable form," which is defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." 44 U.S.C.A. § 3501 note (West 2007).

[80] 44 U.S.C.A. § 3502(8) (West 2007).

[81] NIST, FISMA, Detailed Overview (July 31, 2009), http://csrc.nist.gov/groups/SMA/fisma/overview.html (last visited Oct. 9, 2009).

- "[p]olicies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each [relevant] information system";[82]
- "plans for providing adequate information security for networks, facilities, information systems, or groups of information systems";[83]
- "[s]ecurity awareness training to inform personnel . . . of the information security risks associated with their activities and their responsibilities in complying with . . . policies and procedures designed to reduce these risks";[84]
- "[p]eriodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls";[85]
- "[a] process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices";[86]
- "[p]rocedures for detecting, reporting, and responding to security incidents";[87] and
- "[p]lans and procedures to ensure continuity of operations for information systems."[88]

Heads of agencies are responsible for ensuring that the information security protections implemented by their respective agencies are commensurate with the risk associated with the particular agency's information systems and the information the systems contain.[89] Thus, it is crucial that responsible agency officials understand (1) the "risks . . . that could adversely affect their missions" and (2) the "current status of their security programs and security controls."[90] The ultimate responsibility for authorizing the operation of the agency's information systems and accepting the risk associated with such systems rests with the agency's "authorizing

[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *See* 44 U.S.C.A. § 3544(1)(a) (West 2007).
[90] NIST, FISMA, Detailed Overview, *supra* note 81.

official.'' The authorizing official is a senior management official or agency executive ''with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.''[91]

[2] Legal Requirements

The process of complying with FISMA and NIST regulations consists of the steps discussed below.

1. *Categorize*

Agencies are required to categorize their information systems and the information contained within those systems based on the potential impact, in a hypothetical ''worst case'' scenario, that unauthorized access to or use, disclosure, disruption, modification, or destruction of the agency's information or information systems may have on the integrity, confidentiality, and availability of the information or the information systems.[92] To do so, agencies must first define the *information system boundary,* which means ''a logical group of information resources (information and related resources such as personnel, equipment, funds, and information technology) that have the same function or mission objectives, reside in the same general operating environment, and are under the same direct management control.''[93] Defining the system boundary should permit the agency to identify all information types associated with the information system.

---

[91] National Inst. of Standards & Tech., Federal Information Processing Standards 200, Minimum Security Requirements for Federal Information and Information Systems (2006); *see* National Inst. of Standards & Tech., Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems (2004); National Inst. of Standards & Tech., Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems 12 (2004).

[92] *See* NIST, Categorize Step FAQs (Jan. 27, 2009, Draft), *available at* http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/categorize/faq-categorize-step1.pdf (last visited Oct. 7, 2009) (citing National Inst. of Standards & Tech., Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems (2004); National Inst. of Standards & Tech., Special Publication 800-53, Revision 2, Recommended Security Controls for Federal Information Systems and Organizations (2007)).

[93] *Id.* (citing National Inst. of Standards & Tech., Special Publication 800-39, Managing Risk from Information Systems: An Organizational Perspective (Second Public Draft)

Next, agencies must (1) ''identify the types of information associated with the information system''; (2) assign a security impact value of low,[94] moderate,[95] or high[96] to each type of information for each ''security objective'' (confidentiality,[97] integrity,[98] and availability[99]); (3) assign a security impact value to the system as a whole for each security objective; and (4) determine the overall security impact level for the information system.[100] The security impact value assigned to the system for each security objective is equal to the highest security impact value with respect

29 (2008); National Inst. of Standards & Tech., Special Publication 800-37, Revision 1, Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach (Initial Public Draft) 16-17 (2008)).

[94] ''The potential impact is LOW if . . . [t]he loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.'' National Inst. of Standards & Tech., Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems 2 (2004).

[95] ''The potential impact is MODERATE if . . . [t]he loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.'' *Id.*

[96] ''The potential impact is HIGH if . . . [t]he loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.'' National Inst. of Standards & Tech., Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems 3 (2004).

[97] *Confidentiality* means ''preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. . . .'' 44 U.S.C.A. § 3542 (West 2007). ''A loss of confidentiality is the unauthorized disclosure of information.'' National Inst. of Standards & Tech., Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems 2 (2004).

[98] *Integrity* means ''guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. . . .'' 44 U.S.C.A § 3542. ''A loss of integrity is the unauthorized modification or destruction of information.'' National Inst. of Standards & Tech., Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems 2 (2004).

[99] *Availability* means ''ensuring timely and reliable access to and use of information.'' 44 U.S.C.A. § 3542. ''A loss of availability is the disruption of access to or use of information or an information system.'' National Inst. of Standards & Tech., Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems 2 (2004).

[100] NIST, Categorize Step FAQs (Jan. 27, 2009, Draft), *available at* http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/categorize/faq-categorize-step1.pdf (last visited Oct. 7, 2009).

to that particular security objective assigned to any information type in the system.[101] The system's overall security impact level is classified as low, moderate, or high and is determined by taking the highest security impact value among the system's security objectives.[102] A low-impact information system is one in which all three security objectives have a category of low; a moderate-impact system is one in which at least one security objective is moderate (and none are high); and a high-impact system is one in which at least one security objective is high.[103] For example, an information system that processes some information with a potential impact from loss of confidentiality of high, some information with a potential impact from loss of integrity of moderate (and none at high), and all information with a potential impact from loss of availability of low (and none at moderate or high), will be assigned an impact value of high with respect to confidentiality, moderate with respect to integrity, and low with respect to availability.[104] This hypothetical information system would have a security impact level of high.

The initial security categorization should occur "during the initiation phase of the system development life cycle," along with an initial risk assessment defining the "threat environment in which the information system will operate" and describing the system's basic security needs.[105] After the initial assessment, the agency should regularly reexamine the security impact categorization of its information systems. If a security event occurs, the agency should immediately examine and confirm or alter the security categories of relevant information or information systems and impact level assessments.[106]

NIST guidance details the various types of relevant information and corresponding impact levels. For example, unauthorized access to, use, disclosure, disruption, modification, or destruction of public information may have no security impact with respect to confidentiality and low or

---

[101] *Id.*

[102] *Id.* (citing National Inst. of Standards & Tech., Special Publication 800-53, Revision 2, Recommended Security Controls for Federal Information Systems and Organizations (2007)).

[103] *Id.*

[104] *Id.*

[105] *Id.* (citing National Inst. of Standards & Tech., Special Publication 800-64, Security Considerations in the Information System Development Life Cycle 9–10 (2004)).

[106] *Id.* (citing National Inst. of Standards & Tech., Special Publication 800-53, Revision 2, Recommended Security Controls for Federal Information Systems and Organizations (2007)).

moderate security impact with respect to the integrity and availability of the information (i.e., public information may have a security impact value of N/A with respect to confidentiality, and security impact values of low or moderate with respect to integrity and availability).[107] Information systems containing trade secrets should have a security impact value of at least moderate with respect to confidentiality.[108] NIST guidance suggests that personally identifiable information generally would have at least a moderate security impact value in all three categories.[109] Thus, an information system that contains personally identifiable information likely would have at least a moderate security impact level.

2. *Select*

In the second step, agencies select security controls that correspond with the overall security impact level associated with the information system (determined as set forth above).[110] NIST regulations prescribe the minimum security controls that correspond to the various security impact levels associated with information systems, but agencies may adjust the security control baselines "following the scoping guidance, using compensating controls, and specifying organization-defined parameters."[111] The system's security impact values with respect to each security objective and its overall security impact level also determine the "level of detail to

---

[107] *Id.* (citing 1 National Inst. of Standards & Tech., Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories 28 (2008)). The security impact value of "N/A" is only applicable to the confidentiality security objective (with respect to public information).

[108] *Id.* (citing 1 National Inst. of Standards & Tech., Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories 30 (2008)).

[109] Office of Mgmt. & Budget, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (2003); National Inst. of Standards & Tech., Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems (2004); *see also* National Inst. of Standards & Tech., Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories (2008).

[110] NIST, Categorize Step FAQs, *supra* note 92 (citing National Inst. of Standards & Tech., Special Publication 800-39, Managing Risk from Information Systems: An Organizational Perspective (Second Public Draft) 32 (2008)).

[111] *Id.* (citing National Inst. of Standards & Tech., Special Publication 800-39, Managing Risk from Information Systems: An Organizational Perspective (Second Public Draft) 32 (2008)).

include in security documentation and the level of effort needed to assess the information system."[112] While the requirements for low-impact systems are less onerous than for moderate-impact systems, even the NIST regulations' base-level controls are detailed and extensive.[113]

3. *Implement*

Agencies must implement the selected security controls. If appropriate, agencies should also document their implementation of the security controls, providing a functional description of the implementation (including planned inputs, expected behavior, and expected outputs).[114]

4. *Assess*

Agencies must assess the extent to which the security controls are implemented correctly, operate as intended, and meet the security requirements of the relevant information systems. NIST regulations also refer to this assessment process as "certification."[115]

5. *Authorize*

Agencies must make a decision regarding whether to authorize the operation of the relevant information systems based on the assessment (or "certification") of the risk to the agency or individuals from the operation of the systems and a determination as to whether the risk is acceptable. NIST regulations also refer to this authorization process as "accreditation."[116]

---

[112] *Id.* (citing National Inst. of Standards & Tech., Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems 9–10 (2008)).

[113] *See* National Inst. of Standards & Tech., Federal Information Processing Standards 200, Minimum Security Requirements for Federal Information and Information Systems (2006); National Inst. of Standards & Tech., Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations (2009).

[114] National Inst. of Standards & Tech., Near Real-Time Risk Management (2009), *available at* http://cio.energy.gov/documents/DOE-01-22-2009_Dr_Ross.ppt#1244,40, Authorization Tasks (last visited Aug. 18, 2009).

[115] *See* National Inst. of Standards & Tech., Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems (2008).

[116] *See* National Inst. of Standards & Tech., Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (2004).

Based on the results of the assessment, the authorizing official may: (1) authorize the system, (2) not authorize the system, or (3) grant interim authorization to operate where the authorizing official deems the risk to be unacceptable but there is an overarching mission necessity to place the information system into operation.[117] Where such interim authorization is granted, the agency must implement compensating controls (such as monitoring).

6. *Monitor*

Agencies must monitor and assess selected security controls implemented with respect to relevant information systems on a continuous basis. This includes documenting changes to the system, conducting security impact analyses of the associated changes, and reporting on the security status of the system to appropriate organizational officials on a regular basis.[118] Monitoring must be continuous, with the objective of determining (1) the continued effectiveness of security controls in light of changes in the system and the environment in which the system operates and (2) whether updates to the system are necessary.[119] To be effective, a continuous monitoring process should include at least the following elements:

- [c]onfiguration management and control processes for organizational information systems;
- [s]ecurity impact analyses on actual or proposed changes to information systems and environments of operation;
- [a]ssessment of selected security controls based on a continuous monitoring strategy;
- [s]ecurity status reporting to appropriate organizational officials; and
- [a]ctive involvement by authorizing officials in the ongoing management of information system-related security risks.[120]

---

[117] *See* National Inst. of Standards & Tech., Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems 20.

[118] *See* National Inst. of Standards & Tech., Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (2004); National Inst. of Standards & Tech., Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems (2008).

[119] NIST, Monitor Step FAQs (Jan. 27, 2009, Draft), *available at* http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/monitor/faq_monitor-step6.pdf (last visited Sept. 22, 2009).

[120] *Id.*

[3] Reporting

FISMA requires agencies to file annual reports on the ''adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements'' of the relevant portions of the law.[121] Such reports must be filed with the Director of the Office of Management and Budget, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General.[122]

Additionally, agencies must ''address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports'' relating to certain annual agency budgets, information resources management, information technology management, program performance, financial management, financial management systems, and internal accounting and administrative controls.[123] Agencies also must report any significant deficiencies in relevant policies, procedures, or practices as a ''material weakness'' and, ''if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).''[124]

An Office of Management and Budget (OMB) memorandum released in 2009 requires agencies to report the following information in addition to the statutorily required information set forth above: (1) the agency's breach notification policy ''if it has changed significantly since last year's report,'' (2) ''[p]rogress update on eliminating unnecessary use of Social Security Numbers (SSN),'' and (3) ''[p]rogress update on review and reduction of holdings of personally identifiable information.''[125]

For FISMA reports due in 2009 and thereafter, OMB guidance requires electronic submission through an automated collection tool.[126]

---

[121] 44 U.S.C.A. § 3544(c) (West 2006).

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] Office of Mgmt. & Budget, Memorandum M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (2009); *see also* Office of Mgmt. & Budget, Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (2007).

[126] Office of Mgmt. & Budget, Memorandum M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (2009).

[4] Service Providers

Information services provided by service providers, or ''external information services,'' are not part of the agency's information system.[127] External information services are ''implemented outside of the system's authorization boundary (i.e., services that are used by, but are not a part of, the organization's information systems).''[128]

Service providers that process, store, or house federal government information must comply with all FISMA and related policy requirements. Agencies are responsible and accountable for ensuring the implementation and review of such requirements.[129] Furthermore, agencies must ensure that relevant service providers implement security procedures that are identical to FISMA and NIST requirements, not merely ''equivalent'' thereto.[130] Thus, service providers' ''annual reviews, risk assessments, security plans, control testing, contingency planning, and [NIST certification and accreditation] must, at a minimum, explicitly meet guidance from NIST.''[131] Agencies also are specifically responsible for making sure that service provider personnel receive ''user awareness training and training on agency policy and procedures.''[132]

With respect to relevant information evaluations, such as NIST certification and accreditation and annual IT security self-assessments, the same criteria govern agencies and service providers:

> To the extent that contractor, state, or grantee systems process, store, or house Federal Government information (for which the agency continues to be responsible for maintaining control), their security

---

[127] National Inst. of Standards & Tech., Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations 12–13 (2009).

[128] NIST, Categorize Step FAQs, *supra* note 92.

[129] 44 U.S.C.A. § 3544(a)(1)(A) (West 2007) (''The head of each agency shall [] be responsible for [] providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of . . . information systems used or operated by an agency *or by a contractor of an agency or other organization on behalf of an agency*. . . .'' (emphasis added)).

[130] Office of Mgmt. & Budget, Memorandum M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management 17 (2009).

[131] *Id.*

[132] *Id.*

> controls must be assessed against the same NIST criteria and standards as if they were a Government-owned or -operated system.[133]

To achieve the requisite compliance, agencies are required to "reflect FISMA requirements" in contracts with service providers.[134] Agencies' contracts with service providers should require the latter to (1) "implement and use a configuration management process" for the information systems they operate and manage, (2) "provide regular security status reports that describe the continuous monitoring activities for the information system," and (3) "identify the changes made or planned during the reporting period."[135]

Once established, information systems managed by service providers must be continuously monitored.[136] Authorizing officials and agencies must establish a "trust relationship" with service providers, which relationship will depend on (1) the actions the service providers take to implement security controls that comply with the relevant laws and regulations and any relevant contract or agreement and (2) the service providers' ability to demonstrate that such controls have been properly implemented.[137]

[D] Sarbanes-Oxley Act of 2002

[1] Overview

Congress enacted the Sarbanes-Oxley Act of 2002[138] (SOX) in reaction to prominent corporate and accounting scandals, including those involving Enron, WorldCom, and Arthur Andersen, with the stated purpose of "protect[ing] investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws. . . ."[139] While SOX itself does not directly address information security, it does contain certain requirements that mandate corporate control over

---

[133] FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management at 19.

[134] FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management at 18.

[135] NIST, Monitor Step FAQs, *supra* note 119.

[136] *Id.*

[137] *Id.*

[138] Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 15 U.S.C. and 18 U.S.C.).

[139] *Id.*

information and, as a result, information technology necessary for the effectiveness of such control. Namely, SOX sets forth standards for companies' information controls over financial disclosure (i.e., internal control over financial reporting) as well as disclosure generally (i.e., disclosure controls and procedures).

[2] Corporate Controls over Financial Reporting and Disclosure

[a] Internal Control over Financial Reporting

In section 404 of SOX, Congress directed the SEC to prescribe rules requiring certain registrants subject to Exchange Act reporting requirements to include in their annual reports a report of management on such registrants' internal control over financial reporting (hereinafter Internal Control Report).[140] The SEC's rules for the Internal Control Report[141] define *internal control over financial reporting* as follows:

> [a] process designed by, or under the supervision of, the [registrant's] principal executive and principal financial officers, or persons performing similar functions, and effected by the [registrant's] board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:
>
> (1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the [registrant];
> (2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the [registrant] are being made only in accordance with authorizations of management and directors of the [registrant]; and

---

[140] 15 U.S.C.A. § 7262 (West 2007).

[141] *See* Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Securities Act Release No. 33-8238, Exchange Act Release No. 34-47986, Investment Company Act Release No. IC-26068, 68 Fed. Reg. 36,636 (June 18, 2003).

> (3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the [registrant's] assets that could have a material effect on the financial statements.[142]

As adopted, SEC rules require company management to maintain and evaluate, on an annual basis, the effectiveness of the company's internal control over financial reporting.[143]

Following the annual evaluation, the company must include in its annual report an Internal Control Report containing:

> 1. A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the registrant;
> 2. A statement identifying the framework used by management to evaluate the effectiveness of the registrant's internal control over financial reporting . . . ;
> 3. Management's assessment of the effectiveness of the registrant's internal control over financial reporting as of the end of the registrant's most recent fiscal year, including a statement as to whether or not internal control over financial reporting is effective. This discussion must include disclosure of any material weakness in the registrant's internal control over financial reporting identified by management. Management is not permitted to conclude that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the registrant's internal control over financial reporting; and
> 4. A statement that the registered public accounting firm that audited the financial statements included in the annual report containing the disclosure required [above] has issued an attestation report on the registrant's internal control over financial reporting.[144]

In 2007, the SEC released guidance intended to assist management in its evaluation and assessment of internal controls over financial

---

[142] 17 C.F.R. §§ 240.13a-15(f), 240.15d-15(f). This definition was adopted based in part on a report issued by a committee of the National Commission on Fraudulent Financial Reporting (also known as the Treadway Commission). *See* Committee of Sponsoring Orgs. of the Treadway Comm'n, Internal Control-Integrated Framework (1992) [hereinafter COSO Report].

[143] 17 C.F.R. §§ 240.13a-15(c), 240.15d-15(c) (2008).

[144] 17 C.F.R. § 229.308 (2008); *see also* 17 C.F.R. §§ 240.13a-15(f), 240.15d-15(f).

reporting.[145] In this guidance, the SEC identified information technology general controls as an important factor in an effective system of control over financial reporting risks, noting that "the proper and consistent operation of automated controls or information technology functionality often depends upon effective information technology general controls."[146] For the purpose of providing the Internal Control Report described above, management must design and evaluate the registrant's controls,[147] including its information technology general controls, to ensure that such controls identify all potential risks to financial reporting. Depending on the company, this evaluation may need to include an examination of such broad areas as program development, program changes, computer operations, and access to programs and data.[148]

The registered public accounting firm responsible for preparing the registrant's audit report also must issue an attestation report on the registrant's internal control over financial reporting.[149] To issue such report, the auditors must test and assess the registrant's information systems and other controls, including information access and security controls.[150] SOX section 103 outlines requirements for an auditor's testing of the registrant's internal controls structure and procedures (as required by SOX section 404).[151]

Although the Internal Control Report is an annual requirement, registrants must disclose any material changes in internal controls over financial reporting on a quarterly basis.[152]

In addition to setting forth the foregoing disclosures that registrants must make in their annual and quarterly reports, rules adopted pursuant to

---

[145] Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, Securities Act Release No. 33-8810, Exchange Act Release No. 34-55,929, 72 Fed. Reg. 35,324 (June 27, 2007).

[146] *Id.*

[147] *Id.* (defining *controls* generally as "a specific set of policies, procedures, and activities designed to meet an objective").

[148] *Id.*

[149] *See* 17 C.F.R. §§ 210.2-02(f), 210.1-02(a)(2), 229.308; *see also* 15 U.S.C.A. § 7262(b) (West 2007).

[150] *See generally* Codification of Accounting Standards and Procedures, Statement on Auditing Standards No. 70 (AICPA 1992); PCAOB Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements ¶ B18 (June 12, 2007); *see also* discussion in section 14.02[J].

[151] *See* 15 U.S.C.A. § 7213 (West 2007).

[152] *See* 17 C.F.R. §§ 229.308(c), 240.13a-15(d), 240.15d-15(d) (2008).

section 302 of SOX require that chief executive officers (CEOs) and chief financial officers (CFOs) include personal certifications with respect to internal control over financial reporting in all annual and quarterly reports.[153]

CEOs and CFOs must certify, with respect to internal control over financial reporting, that they are personally responsible for establishing and maintaining internal control over financial reporting and have:

> 1. Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under [their] supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles; . . . [and]
> 2. Disclosed in [the] report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting.[154]

CEOs and CFOs must also certify that they have disclosed to the company's auditors and the audit committee of the board of directors "[a]ll significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information" and "[a]ny fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting."[155]

[b] Disclosure Controls and Procedures

Similar to the disclosures and certifications required with respect to internal control over financial reporting, registrants and their CEOs and CFOs must provide disclosures and certifications as to the effectiveness of the registrants' disclosure controls and procedures. Disclosure controls

---

[153] *See* 15 U.S.C.A. § 7241 (West 2007); *see also* 17 C.F.R. §§ 240.13a-14(a), 240.15d-14(a) (2008). The content of the certifications is set out in 17 C.F.R. § 229.601 (2008).

[154] 17 C.F.R. § 229.601 (2009).

[155] *Id.*

and procedures encompass all company disclosure, including but not limited to financial reporting. The term *disclosure controls and procedures* is defined as:

> controls and other procedures of [a registrant] that are designed to ensure that information required to be disclosed by the [registrant] in the reports that it files or submits under the [Exchange Act] is recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by [a registrant] in the reports that it files or submits under the Act is accumulated and communicated to the [registrant's] management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure.[156]

A registrant must disclose, in each quarterly and annual report, its management's conclusions regarding the "effectiveness of the registrant's disclosure controls and procedures" as of the end of the quarter or year covered by the report.[157]

A registrant's CEO and CFO also must include personal certifications with respect to disclosure controls and procedures in all annual and quarterly reports, in addition to the certifications regarding internal control over financial reporting described above.[158]

CEOs and CFOs must certify, with respect to disclosure controls and procedures, that they are responsible for establishing and maintaining disclosure controls and procedures and have:

> 1. Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under [their] supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to [them] by others within those entities, particularly during the period in which [the] report is being prepared; . . . [and]
> 2. Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in [the] report [their] conclusions

---

[156] 17 C.F.R. §§ 240.13a-15(e), 240.15d-15(e) (2008).

[157] 17 C.F.R. § 229.307 (2008); *see also* 17 C.F.R. §§ 240.13a-15(b), 240.15d-15(b).

[158] *See* 17 C.F.R. §§ 240.13a-14(a), 240.15d-14(a) (2008). The content of the certifications is set out in 17 C.F.R. § 229.601 (2008).

> about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by [the] report based on such evaluation. . . .[159]

[3] Liability for Ineffective Information Controls

Under the foregoing SOX rules, and in light of the related SEC guidance, effective internal control over financial reporting as well as disclosure controls and procedures depend on effective information controls. Both the company and its certifying officers may face liability if ineffective information controls prevent the company and its officers from providing the required SOX certifications and disclosures or render their certifications false. Violations of SOX are treated in a similar manner as other violations of the securities laws, and may result in injunctions, civil monetary penalties, director and officer bans, and, in some cases, criminal fines and imprisonment.[160] Furthermore, because the disclosures and certifications described above are required to be filed with the relevant annual or quarterly reports, a registrant's inability to provide the required certifications may result in the late filing of such a report. Failing to file an annual or quarterly report on time may cause the registrant to lose Form S-3 eligibility, which will constrain the registrant in its ability to offer and sell securities to the public.[161] Additionally, the failure to provide required certifications as described above may result in actions as grave as delisting by a securities exchange.[162] Finally, registrants face significant reputational risks for any SOX violations.

[E] Red Flags Rule[163]

[1] Overview

The Identity Theft Red Flags and Address Discrepancies Rule implements sections 114 and 315 of the Fair and Accurate Credit Transactions

---

[159] 17 C.F.R. § 229.601 (2008).

[160] 15 U.S.C.A. § 7202(b) (West 2007); *see also* 15 U.S.C.A. § 78u. Officers who provide false certifications with respect to filed financial statements' accuracy and compliance with applicable laws and regulations may also face personal criminal liability. *See* 18 U.S.C.A. § 1350 (West 2007).

[161] *See* Form S-3, Fed. Sec. L. Rep. (CCH) ¶¶ 7151–7160, at 7152 (2009).

[162] *See, e.g.*, NYSE, Inc., Listed Company Manual §§ 802.01D, 802.01E (2009).

[163] For more information on the Red Flags Rule, see section 2.03[D].

Act of 2003 (FACTA).[164] The Red Flags Rule was promulgated jointly by the FTC and certain federal functional regulators (i.e., the Federal Reserve, Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and NCUA).[165] The Rule requires ''financial institutions'' and ''creditors'' (as those terms are defined in FACTA) that offer or maintain certain accounts to develop and implement a written identity theft prevention program. In addition, the Red Flags Rule requires users of consumer reports issued by nationwide consumer reporting agencies (CRAs) to implement procedures for handling notices of address discrepancy that they receive from the CRAs.[166] In addition, credit and debit card issuers are required to implement procedures for assessing the validity of change of address notifications. The compliance deadline was November 1, 2008.[167] For entities subject to the FTC's enforcement jurisdiction, the FTC delayed until November 1, 2010, the enforcement of the provisions of the Red Flags Rule requiring the implementation of an identity theft prevention program.[168]

[2] Covered Entities

The Red Flags Rule's requirement to implement an identity theft prevention program applies to financial institutions and creditors.[169] For purposes of the Rule, the term *financial institutions* encompasses (1) state or national banks, state or federal savings and loan associations and credit unions, and mutual savings banks; and (2) any entity that, directly or indirectly, holds a deposit or account belonging to a consumer, from which

---

[164] *See* 15 U.S.C.A §§ 1681m(e), 1681c(h) (West 2007). For more information on FACTA, see section 2.03.

[165] *See, e.g.*, FTC Red Flags Rule, 16 C.F.R. §§ 641.1, 681.1–681.2 (2008); Federal Reserve Red Flags Rule, 12 C.F.R. §§ 222.82, 222.90, 222.91 (2008); FDIC Red Flags Rule, 12 C.F.R. §§ 334.82, 334.90, 334.91 (2008).

[166] *Nationwide consumer reporting agencies* (CRAs) are agencies that regularly engage in the practice of assembling or evaluating, and maintaining public record information and credit account information for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity. *See* 15 U.S.C.A. § 1681a(p) (West Supp. 2007). Examples of CRAs include Equifax, Experian, and TransUnion.

[167] *See* 72 Fed. Reg. 63,718 (Nov. 9, 2007).

[168] Press Release, FTC Announces Expanded Business Education Campaign on ''Red Flags'' Rule (July 29, 2009), http://www.ftc.gov/opa/2009/07/redflag.shtm.

[169] *See* 16 C.F.R. § 681.1(a) (2009).

the consumer may withdraw funds to make payments or transfers to third parties or others, or from which the consumer may make payments to third parties at an automated teller machine, a remote service unit, or other electronic device.[170] The term *creditors* means entities that regularly extend, renew, arrange for, or continue credit.[171] The requirement to implement an identity theft prevention program applies not only to businesses but also to nonprofit entities and government agencies that act as ''financial institutions'' or ''creditors.''

Not every financial institution or creditor is required to establish an identity theft prevention program. Rather, this requirement applies only to entities that offer or maintain (1) consumer accounts that involve multiple transactions, or (2) other accounts that are associated with a reasonable risk of harm to the entity or its customers from identity theft. In practice, the Red Flags Rule requires most financial institutions and creditors that offer or maintain most consumer accounts to implement an identity theft prevention program. Financial institutions and creditors that offer or maintain other accounts (such as business accounts) have the discretion under the Rule to determine whether such accounts must be covered by the program.

[3] Identity Theft Prevention Program

The Red Flags Rule defines *identity theft* as ''fraud that is committed or attempted using identifying information of another person without authority.''[172] Accordingly, the Rule may be best viewed as a fraud prevention mandate. Often, rather than attempting to steal an identity, the perpetrator is using personal information he has stolen or otherwise obtained unlawfully to commit fraud. It is important to keep in mind that the purpose of the Red Flags Rule (and specifically, the identity theft prevention program) is to enable businesses to detect the tell-tale signs of this type of fraud (i.e., ''Red Flags''), develop response mechanisms that enable businesses to effectively prevent such fraud (after its signs are detected), and mitigate the damage the fraud may cause.

The Red Flags Rule does not articulate specific requirements for the identity theft prevention program's form or content but instead sets forth

---

[170] *See* 15 U.S.C.A § 1681(t) (West 2007); 12 U.S.C.A § 461(b)(1)(C) (West 2007); 12 C.F.R. § 204.2(e) (2009).

[171] *See* 15 U.S.C.A §§ 1681a(r)(5), 1691a(d), (e) (West 2007).

[172] *See* 16 C.F.R. §§ 681.1(b)(8), 603.2(a) (2009).

the process that organizations must follow in developing, implementing, and administering an identity theft prevention program tailored to the entities' size and complexity and the nature of their operations. The Rule requires entities to (1) identify patterns, practices, and activities that indicate the possible existence of identity theft in connection with relevant accounts the entity offers or maintains; and (2) develop methods for detecting and responding to those Red Flags.[173]

[4] Other Requirements

Covered entities are also required to (1) train relevant personnel to implement the program effectively; (2) take steps to ensure that relevant service providers conduct their activities in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft;[174] and (3) periodically evaluate the effectiveness of the program and appropriately update the program to reflect the entities' own experiences with identity theft issues as well as changes in relevant business arrangements and known methods of identity theft.[175] The Red Flags Rule requires entities that use consumer reports provided by a nationwide CRA to implement reasonable policies and procedures for handling notices of address discrepancy.[176] A CRA issues a notice of address discrepancy when the address provided in a request for a consumer report substantially differs (as determined by the CRA) from addresses the agency has on file for the relevant individual.

Responding to a notice of address discrepancy requires users to (1) verify that the consumer report relates to the individual about whom the report was requested, and, in certain circumstances, (2) confirm and

---

[173] *See* 16 C.F.R. § 681.1(c)–(e) (2009).

[174] Such steps may include contractually requiring the service providers to (1) maintain policies and procedures to detect Red Flags relevant to the functions they perform, and (2) either report the Red Flags to the covered entity when they are detected or take appropriate steps to prevent and mitigate identity theft in response to the detected Red Flags. The Red Flags Rule also directs that relevant service providers be required to periodically submit to audits of their identity theft policies and procedures. This requirement is not explicitly stated in the Rule but is instead based on the requirements the Rule imposes on covered entities to (1) consider service provider oversight arrangements in the risk assessment conducted for periodic identification of covered accounts, and (2) address service provider oversight arrangements in periodic compliance reports.

[175] *See* 16 C.F.R. § 681 app. A (2009).

[176] *See* 16 C.F.R. § 641.1 (2009).

provide to the relevant CRA the individual's accurate address.[177] Users must provide the relevant individual's accurate address to the CRA that issued the notice when (1) it has been reasonably confirmed that the consumer report relates to the individual about whom the report was requested, (2) the entity has established a continuing relationship with the relevant individual, and (3) the entity regularly and in the ordinary course of business furnishes information to the CRA from which it received the notice of address discrepancy.[178] The accurate address should be provided to the CRA as part of the information the entity regularly furnishes for the reporting period.[179]

Users of consumer reports should confirm that they have implemented procedures not only for handling notices of address discrepancy but also for recognizing and detecting the notices when they are included in consumer reports. It may not always be apparent that a consumer report includes a notice of address discrepancy. The format of the notice varies among the CRAs, with at least one of the agencies including only a ''yes'' or ''no'' field in its consumer reports, with a ''yes'' denoting the agency's determination that there is a substantial difference between the address in the request the agency received and the addresses it has on file for the individual.[180]

The Red Flags Rule requires issuers of credit or debit cards to establish reasonable policies and procedures for assessing the validity of change of address notifications that issuers receive in connection with payment card accounts.[181] When a notification is followed within 30 days by a request for an additional or replacement payment card, the Rule prohibits issuers from providing the customer with a card until the change of address is verified.[182]

The Red Flags Rule provides two methods for verifying the validity of change of address notifications.[183] First, the issuer may comply with the Rule by notifying the cardholder of the change of address notification and providing the cardholder with reasonable means of reporting an incorrect

---

[177] *See* 16 C.F.R. § 641.1(c), (d) (2009).

[178] *Id.*

[179] *See* 16 C.F.R. § 641.1(d)(3) (2009).

[180] *See* SR 08-7/CA 08-10, Interagency Examination Procedures (Oct. 10, 2008); Section 615(e) Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft (12 C.F.R. § 222.90).

[181] *See* 16 C.F.R. § 681.2 (2009).

[182] *See* 16 C.F.R. § 681.2(c) (2009).

[183] *See* 16 C.F.R. § 681.2(c), (d) (2009).

notification, as provided in the Rule.[184] Second, an issuer may assess the validity of a change of address notification pursuant to procedures it develops and maintains in connection with its identity theft prevention program.[185] Incorporating this assessment into the program obviates the need for further verification of the change of address and avoids delay in issuing additional or replacement payment cards. Using this method, when an issuer receives a change of address notification, it would examine the notification for the presence of relevant Red Flags.[186] If no Red Flags are detected or the detected Red Flags are resolved to the issuer's satisfaction, the issuer may implement the change of address and subsequently issue a new or additional payment card without delay.[187] Issuers may comply with the requirements of this provision by verifying the validity of a change of address notification at the time the issuer receives the notification.[188] This approach obviates, for purposes of this provision of the Red Flags Rule, the need to monitor if a cardholder requests an additional or replacement card following the notification of change of address.

[F] Records Disposal Laws

There are numerous federal and state laws that require the secure disposal of hard-copy and electronic records that contain personal information. Below is an overview of these requirements.

[1] Federal Trade Commission Disposal Rule

In 2004, the FTC promulgated regulations requiring businesses to properly dispose of certain consumer information.[189] The FTC enacted the Disposal Rule pursuant to FACTA.[190] The Disposal Rule is designed to help combat identity theft resulting from the improper disposal of consumer report information.[191] It is intended to protect consumer privacy and prevent fraud by requiring companies to take reasonable steps to guard

[184] 16 C.F.R. § 681.2(c)(1) (2009).
[185] 16 C.F.R. § 681.2(c)(2) (2009).
[186] 16 C.F.R. § 681.1 (2009).
[187] *Id.*
[188] 16 C.F.R. § 681.2(d) (2009).
[189] 16 C.F.R. pt. 682 (2008) [hereinafter Disposal Rule].
[190] Pub. L. No. 108-159, 111 Stat. 1952 (codified as amended in scattered sections of 15 U.S.C.).
[191] 16 C.F.R. § 682.2 (2008).

against unauthorized access to or use of consumer report information in connection with its disposal.[192] In addition to CRAs, entities affected by the Rule include lenders, insurers, employers, landlords, mortgage brokers, car dealers, and other businesses that use consumer reports.[193]

The Disposal Rule applies to any business that maintains or otherwise possesses "consumer information."[194] *Consumer information* means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report (including compilations of these records).[195] A *consumer report,* as defined by the Fair Credit Reporting Act (FCRA), is any written, oral, or other communication of any information by a CRA bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or collected as a factor in establishing the consumer's eligibility for:

1. "credit or insurance to be used primarily for personal, family, or household purposes";
2. "employment purposes"; or
3. "any other permissible purpose authorized under [the FCRA]."[196]

Information that does not identify individuals, such as aggregate or blind data, is not covered by the Disposal Rule. The Disposal Rule requires covered entities to properly dispose of consumer information "by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[197] *Disposal* includes:

1. discarding or abandoning consumer information; or
2. selling, donating, or transferring any medium, including computer equipment, on which consumer information is stored.[198]

---

[192] *See id.; see also* FTC Business Alert, Disposing of Consumer Report Information? New Rule Tells How (June 2005), *available at* http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt152.shtm (last visited Oct. 2, 2009).

[193] FTC Business Alert, Disposing of Consumer Report Information? New Rule Tells How, *supra* note 192.

[194] 16 C.F.R. § 682.3.

[195] 16 C.F.R. § 682.1(b) (2008).

[196] 15 U.S.C.A. § 1681a (West 2007).

[197] 16 C.F.R. § 682.3(a) (2008).

[198] 16 C.F.R. § 682.1(c).

The Disposal Rule does not define what is "reasonable," instead allowing for a flexible standard that permits covered entities to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and relevant changes in technology over time.[199] The Rule includes specific examples of measures the FTC believes satisfy the Rule's disposal standard.[200] These examples, which are intended as guidance and not as a safe harbor or exclusive methods for compliance, include:

1. implementing policies and procedures that require (a) the burning, pulverizing, or shredding of papers containing consumer information; and (2) the destruction or erasure of electronic media containing consumer information, so the information cannot practicably be read or reconstructed;
2. conducting due diligence of a disposal company under consideration (which due diligence could include conducting an independent audit of the company's operations, obtaining references, or requiring that the disposal company be certified) and entering into a contract with the disposal company to dispose of consumer information in a manner consistent with the Disposal Rule;
3. for disposal companies, implementing policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with the first example set forth above; and
4. for entities subject to GLB's Safeguards Rule,[201] incorporating the proper disposal of consumer information as required by the Disposal Rule into the information security program required by the Safeguards Rule.[202]

[2] State Records Disposal Laws

Several states have laws that address the disposal of records containing personal information.[203] These state law requirements are summarized

---

[199] FTC Business Alert, Disposing of Consumer Report Information? New Rule Tells How, *supra* note 192.

[200] 16 C.F.R. § 682.3(b).

[201] 16 C.F.R. pt. 314.

[202] 16 C.F.R. § 682.3(b).

[203] *See, e.g.*, Ark. Code Ann. § 4-110-104 (LEXIS 2009); Cal. Civ. Code § 1798.81 (West, Westlaw 2010); Ga. Code Ann. § 10-15-2 (LEXIS 2009); Tex. Bus. & Com. Code

in the chart "Selected State Records Disposal Laws" located in Appendix C. Generally, these state laws require organizations to take reasonable steps to securely dispose of hard-copy or electronic records containing personal information by one of the following methods: (1) shredding, (2) erasing, or (3) modifying the personal information so it is unreadable. Organizations should review their records management programs to ensure that they are updated to reflect relevant state records disposal laws. In some cases, these laws provide a private right of action to individuals.[204]

[G] State Information Security Laws

A number of states have enacted laws that require organizations that maintain personal information about state residents to adhere to general information security requirements with respect to that personal information.[205] Numerous states also have passed laws specifically regulating organizations' use of Social Security numbers (SSNs).[206] In addition, Massachusetts and Nevada have enacted information security laws that impose highly prescriptive requirements on organizations with respect to the processing of personal information. State information security requirements are summarized in the chart "Selected State Information Security Laws," found in Appendix B. Below is a general overview of certain prominent state information security regimes.

[1] California's Information Security Law and Analogous State Laws

As with several state privacy initiatives, California became the first state to impose a general information security standard on businesses that maintain personal information.[207] Other states (such as Arkansas, Connecticut, Maryland, Nevada, Oregon, Rhode Island, Texas, and Utah) have

---

Ann. §§ 72.001–72.051 (Vernon, Westlaw 2009); Wash. Rev. Code Ann. § 19.215.020(1) (LEXIS 2009); *see generally* Appendix C.

[204] *See, e.g.*, Cal. Civ. Code § 1798.84 (West, Westlaw 2010) (providing that "[a]ny customer injured by a violation of this title may institute a civil action to recover damages").

[205] For more information on state information security laws, see Appendix B.

[206] *See* Appendix D.

[207] Cal. Civ. Code § 1798.81.5 (West, Westlaw 2009).

followed suit, enacting their own information security laws requiring companies to implement reasonable information security measures.[208] Below is a discussion of the California law, which is representative of the other general state information security laws.

Section 1798.81.5 of the California Civil Code requires businesses that own or license personal information about California residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, destruction, use, modification, or disclosure.[209] The law does not define what is ''reasonable,'' nor does it offer guidance on how to meet the reasonableness standard. This means covered businesses must define internally the security measures they consider both reasonable and appropriate in light of the scope of their operations and the nature and sensitivity of the personal information they maintain. In addition, businesses that disclose personal information to nonaffiliated third parties must contractually require those entities to maintain reasonable security procedures.[210] Thus, covered businesses must keep track of third-party recipients of personal information (such as service providers) and require them by contract to implement appropriate security measures. Given the geographic reach of many businesses, this California law effectively imposes a national standard on businesses that maintain personal information.

The law applies to all businesses (other than those described below) that own or license personal information about California residents.[211] Personal information that is ''own[ed] or license[d]'' includes (but is not limited to) personal information that a business retains as part of its internal customer account or for use in transactions with the person to whom the information relates.[212] Similar to the definition found in the California state security breach notification law, *personal information* is defined in

---

[208] *See, e.g.*, Ark. Code Ann. §§ 4-110-101 to 4-110-108 (LEXIS 2009); Cal. Civ. Code § 1798.81.5 (West, Westlaw 2009); Conn. Gen. Stat. Ann. § 42-471 (West, Westlaw 2010); Md. Code Ann., Com. Law §§ 14-3501 to 14-3503 (LEXIS 2009); Nev. Rev. Stat. § 603A.210 (LEXIS 2009); Or. Rev. Stat. § 646A.622 (West, Westlaw 2009); R.I. Gen. Laws § 11-49.2-2 (LEXIS 2008); Tex. Bus. & Com. Code Ann. §§ 72.001–72.051 (West, Westlaw 2009); Utah Code Ann. §§ 13-44-101 to 13-44-301 (LEXIS 2009).

[209] Cal. Civ. Code § 1798.81.5 (West, Westlaw 2009).

[210] *Id.*

[211] *Id.*

[212] *Id.*

the California security law to mean unencrypted data consisting of a person's name, in combination with:

1. a Social Security number;
2. a driver's license or California identification card number;
3. an account, credit card, or debit card number along with a password or access code; or
4. medical information.[213]

The law excludes from coverage entities that are subject to HIPAA and California's medical, financial, and motor vehicle records privacy laws.[214] In addition, any business that complies with another state or federal law providing greater protection to personal information is deemed to be in compliance with the law.

[2] State Social Security Number Laws

A number of state laws prohibit (1) intentionally communicating SSNs to the general public, (2) using SSNs on ID cards required for individuals to receive goods or services, (3) requiring that SSNs be used in Internet transactions unless the transaction is secure or the SSN is encrypted or redacted, (4) requiring an individual to use an SSN to access a Web site unless another authentication device is also used, and (5) mailing materials with SSNs (subject to certain exceptions, including requirements of state or federal law).[215] Some of these state laws provide exemptions for entities that used SSNs continuously in the enumerated

---

[213] *Id.*

[214] *Id.*

[215] *See, e.g.*, Ariz. Rev. Stat. § 44-1373 (West, Westlaw 2009); Cal. Civ. Code § 1798.85 (West, Westlaw 2009); Colo. Rev. Stat. § 6-1-715 (LEXIS 2008); Haw. Rev. Stat. Ann. §§ 487J-2 to 487J-3 (LEXIS 2009); 815 Ill. Comp. Stat. Ann. 505/2RR, 505/2QQ (LEXIS 2009); Md. Code Ann., Com. Law §§ 14-3401 to 14-3403 (Michie, LEXIS 2009); Mich. Comp. Laws Serv. §§ 445.81–445.87 (LEXIS); Minn. Stat. Ann. § 325E.59 (West, Westlaw 2009); N.J. Stat. Ann. § 56:8-164 (West, Westlaw 2009); N.Y. Gen. Bus. Law § 399-dd (McKinney, Westlaw 2009); N.C. Gen. Stat. § 75-62 (LEXIS 2008); Okla Stat. Ann. tit. 40, § 173.1 (West, Westlaw 2009); Pa. Stat. Ann. § 201 (Purdon, Westlaw 2009); R.I. Gen. Laws § 6-48-8 (LEXIS 2008); S.C. Code Ann. § 37-20-180 (West, Westlaw 2008); Tex. Bus. & Com. Code Ann. § 501.002 (Vernon, Westlaw 2009); Vt. Stat. Ann. tit. 9, § 2440 (LEXIS 2008). For further details regarding state SSN laws, see Appendix D.

ways before the relevant laws' enactment.[216] Grandfathered entities must notify individuals of their right to opt out of using their SSN.[217] In addition to the restrictions on SSNs enumerated above, certain states have enacted laws that impose similar, but less comprehensive, restrictions on the use of SSNs.[218] State law requirements regarding the use of SSNs are summarized in the "Selected State Social Security Number Protection Laws" chart, located in Appendix D.

A number of state laws impose restrictions targeting specific SSN uses. Missouri law, for example, prohibits organizations from requiring an individual to use his or her SSN as an employee identification number for any type of employment-related activity, subject to an exception for internal verification or administrative purposes.[219] Subject to certain exceptions, New Mexico law limits a business's ability to transmit an SSN in conjunction with an account number to a narrow set of circumstances, including for certain application, enrollment, or termination processes.[220] In New York, employers are prohibited from placing an SSN in files with unrestricted access.[221]

A few states have chosen to allow redacted SSNs to be used in certain circumstances. Health ID cards in Washington must not display more than four digits of an individual's SSN.[222] California labor law requires

---

[216] *See, e.g.*, Ariz. Rev. Stat. § 44-1373 (West, Westlaw 2009); Colo. Rev. Stat. § 6-1-715 (LEXIS 2008); 815 Ill. Comp. Stat. Ann. 505/2RR, 505/2QQ (LEXIS 2009); 74 Pa. Stat. Ann. § 201(c) (LEXIS 2009); Tex. Bus. & Com. Code Ann. § 501.002 (Vernon, Westlaw 2009); Vt. Stat. Ann. tit. 9, § 2440 (LEXIS 2008).

[217] *See, e.g.*, Ariz. Rev. Stat. § 44-1373 (West, Westlaw 2009); Colo. Rev. Stat. § 6-1-715 (LEXIS 2008); 815 Ill. Comp. Stat. Ann. 505/2RR, 505/2QQ (LEXIS 2009); 74 Pa. Stat. Ann. § 201(c) (LEXIS 2009); Tex. Bus. & Com. Code Ann. § 501.002 (Vernon, Westlaw 2009); Vt. Stat. Ann. tit. 9, § 2440 (LEXIS 2008).

[218] *See, e.g.*, Alaska Stat. § 45.48.400 (LEXIS 2008), Ark. Code Ann. § 4-86-107 (LEXIS 2009); Conn. Gen. Stat. Ann. § 42-470 (West, Westlaw 2010); Ga. Code Ann. § 10-1-393.8 (LEXIS 2009); Mo. Ann. Stat. § 407.1355 (West, Westlaw 2009); N.M. Stat. Ann. § 57-12B (West, Westlaw 2009); Or. Rev. Stat. Ann. § 646A.620 (West, Westlaw 2009); S.D. Codified Laws § 1-27-44 (West, Westlaw 2009) and Sup. Ct. R. 09-06; Tenn. Code Ann. § 47-18-2110 (LEXIS 2008); Utah Code Ann. § 13-45-301 (LEXIS 2009); Va. Code Ann. § 59.1-443.2 (LEXIS 2009). For further details regarding these state SSN laws, see Appendix D.

[219] *See* Mo. Ann. Stat. § 407.1355(4) (West, Westlaw 2009).

[220] *See* N.M. Stat. Ann. § 57-12B-4(4) (West, Westlaw 2009).

[221] *See* N.Y. Lab. Law § 203-d (McKinney, Westlaw 2009). The New York law also defines *Social Security account number* to include "the number issued by the federal social security administration and any number derived from such number." *Id.*

[222] Wash. Rev. Code Ann. § 48.43.022 (West, Westlaw 2009).

employers to use no more than four digits of an employee's SSN on checks or vouchers.[223] In some states, legal restrictions apply even where there is not a full nine-digit SSN but instead a number derived from an SSN, such as the last four digits.[224]

There is a growing trend at the state level to require (1) encryption of SSNs and (2) the publication by companies of dedicated SSN protection policies. In addition, as discussed in more detail below, Massachusetts and Nevada have requirements mandating the encryption of SSNs in transit.[225] In Nevada, the law specifies technological standards for the encryption of SSNs in transit.[226]

With respect to corporate SSN policies, Connecticut, Michigan, and Texas require organizations to create and publish policies regarding their collection and use of SSNs. In Connecticut, for example, the law requires a policy that (1) protects the confidentiality of SSNs, (2) prohibits unlawful disclosure of SSNs, and (3) limits access to SSNs.[227] The laws in Michigan and Texas are similar to the SSN law in Connecticut.[228]

[3] Massachusetts Standards for the Protection of Personal Information

In 2008, Massachusetts issued regulations requiring any person who holds personal information about Massachusetts residents to develop and implement a comprehensive, written information security program to

---

[223] Cal. Lab. Code § 226 (West, Westlaw 2009). .

[224] *See, e.g.*, Mich. Comp. Laws Ann. § 445.83 (West, Westlaw 2009) (applying these restrictions to the last four digits of the SSN); N.Y. Gen. Bus. Law § 399-dd (McKinney, Westlaw 2009) (defining the SSN to include any number derived from an individual's SSN).

[225] *See* 201 Mass. Regs. Code § 17.04 (2009); S.B. 227, 75th Leg., Reg. Sess. (Nev. 2009) (to be codified at Nev. Rev. Stat. § 603A). For purposes of the Massachusetts regulations, encryption is required for "all transmitted records and files containing personal information that will travel across public networks" and for "all data containing personal information to be transmitted wirelessly." 201 Mass. Regs. Code § 17.04.

[226] *See* 201 Mass. Regs. Code § 17.04 (2009); S.B. 227, 75th Leg., Reg. Sess. (Nev. 2009) (to be codified at Nev. Rev. Stat. § 603A). For purposes of the Nevada law, data are in transit when they are transferred "through an electronic, nonvoice transmission other than a facsimile. . . ." S.B. 227, 75th Leg., Reg. Sess. (Nev. 2009).

[227] *See* Conn. Gen. Stat. Ann. § 42-471 (West, Westlaw 2010).

[228] *See* Mich. Comp. Laws Ann. § 445.84 (West, Westlaw 2009); Tex. Bus. & Com. Code Ann. § 501.052 (Vernon, Westlaw 2009).

protect the data.[229] Prior to taking effect, the regulations were amended in February 2009 and again in August 2009. The regulations apply in the context of both consumer and employee information, and require the protection of personal data in both paper and electronic formats.[230] They impose stringent and comprehensive data security standards on all businesses with Massachusetts consumers or employees.[231] Massachusetts was the first state in the nation to adopt such comprehensive information security requirements applicable to all types of organizations. As a result of the August 2009 amendments, the deadline for compliance was March 1, 2010.[232]

The regulations apply to "persons who own or license personal information about a resident of the Commonwealth of Massachusetts."[233] *Person* is defined broadly to include natural persons, corporations, and other legal entities.[234] *Personal information* is defined as

> a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.[235]

Personal information does not include data that are publicly available.[236] As indicated above, the standards require safeguards for personal information maintained in either paper or electronic records.[237] The regulations apply to all private entities, regardless of size or industry sector, that hold personal information about Massachusetts residents.[238]

Businesses with Massachusetts consumers or employees are required under the regulations to develop and implement a "comprehensive

---

[229] 201 Mass. Regs. Code §§ 17.01–17.05 (2008).
[230] 201 Mass. Regs. Code § 17.03.
[231] *Id.*
[232] 201 Mass. Regs. Code § 17.05.
[233] 201 Mass. Regs. Code § 17.01.
[234] 201 Mass. Regs. Code § 17.02.
[235] *Id.*
[236] *Id.*
[237] 201 Mass. Regs. Code § 17.01.
[238] *See id.*

information security program that is written in one or more readily accessible parts."[239] The regulations establish minimum standards to safeguard personal information, including:

1. designating one or more employees to maintain the information security program;
2. identifying and assessing internal and external security risks and the effectiveness of current safeguards, and upgrading safeguards as necessary;
3. restricting physical access to records containing personal information;
4. securing the records and data in locked facilities, storage areas, or containers;
5. regularly monitoring employee access to personal information;
6. reviewing security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information, and taking corrective action when indicated by the review process; and
7. documenting actions taken in response to security breaches, with a mandatory post-incident review of events and actions taken, if any, to make changes in business practices.[240]

Under the regulations, businesses must contract with service providers in addition to taking reasonable steps to "select and retain third-party service providers that are capable of maintaining appropriate security measures to protect . . . personal information. . . ."[241] Information security programs implemented pursuant to the standards must require, to the extent technically feasible, encryption of all personal information that (1) will travel across public networks, (2) is transmitted wirelessly, and (3) is "stored on laptops or other portable devices."[242]

[239] 201 Mass. Regs. Code § 17.03.
[240] *Id.*
[241] *Id.*
[242] 201 Mass. Regs. Code § 17.04.

Businesses that store or transmit such personal information electronically also must:

1. establish user authentication protocols that include control of user IDs and a secure method of assigning passwords (including prohibiting use of vendor-supplied default passwords);
2. maintain reasonably up-to-date operating system security patches, firewalls, anti-malware programs, and virus definitions;
3. ensure that password location does not compromise the security of the data it protects, that access to the system via password is restricted to active users only, and that access is blocked after multiple unsuccessful attempts of using a password; and
4. engage in periodic system monitoring for signs of unauthorized use or access.[243]

[4] Nevada Encryption Law for the Transmission of Personal Information

In 2005, Nevada enacted a law requiring businesses to encrypt customer personal information if those data are transmitted electronically outside a business's "secure system," other than via facsimile.[244] In passing this law, Nevada became the first state to specifically mandate encryption as a technical safeguard. The state enacted a new information security law in 2009 that repealed the 2005 law. The 2009 law requires that organizations doing business in Nevada (that do not collect payment card data) use encryption when (1) transferring "any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector," and (2) moving "any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor. . . ."[245] A *data storage device* is any device that stores information or data from any electronic or optical medium, including, but not limited to, computers, cellular telephones, magnetic tape, electronic computer drives, optical computer drives, and the medium itself.[246]

---

[243] *Id.*

[244] Nev. Rev. Stat. Ann. § 597.970 (repealed 2009).

[245] S.B. 227, 2009 Leg., 75th Sess. (Nev. 2009) (to be codified at Nev. Rev. Stat. § 603A).

[246] *Id.*

For those organizations doing business in Nevada that do collect payment card data, the 2009 law mandates that they comply with the Payment Card Industry Data Security Standard (PCI DSS).[247] In this regard, the law essentially codifies standard industry practice for businesses that accept payment cards. While Minnesota law[248] codifies selected PCI DSS requirements, the Nevada law is significantly more comprehensive as it adopts by reference the PCI DSS in its entirety. In all cases, an entity that complies with the Nevada law is not liable for damages resulting from a security breach, provided that the security breach is not caused by the gross negligence or intentional misconduct of the business, or its officers, employees, or agents.[249] The effect of the law is to create a potential safe harbor against liability for damages resulting from a security breach.

[H] Anti-Spyware Laws

[1] Overview

Spyware is a vaguely defined term that includes many different types of computer software.[250] A 2005 FTC report addressed the difficulties in defining the term.[251] The report identified the various challenges to reaching a consensus regarding the definition, including: (1) issues concerning how, what, and when consumers need to be told about software downloaded or installed on their computers for consent to such download

---

[247] *Id.*

[248] Minn. Stat. Ann. § 325E.64(22) (West, Westlaw 2009). The Minnesota law makes it unlawful for any person or entity conducting business in Minnesota that accepts payment cards to retain the card security code, the PIN verification code, or the full contents of any track or magnetic stripe data following the authorization of the transaction. In the case of a PIN debit transaction, the law makes it unlawful to retain such data more than 48 hours after the transaction. The same is true for any service provider retained by the business to process transactions on its behalf.

[249] S.B. 227, 2009 Leg., 75th Sess. (Nev. 2009) (to be codified at Nev. Rev. Stat. § 603A).

[250] Definition of the term is a contentious issue in part because of the risk that any legislation that incorporates an overly broad term may go too far in chilling legitimate business activities and potentially could impede freedom of speech or other Constitutional guarantees. *See* WhenU.com Inc. v. Utah, No. 040907578 (Utah Dist. Ct. June 22, 2004) (granting a preliminary injunction of the law to plaintiff adware provider on the ground that the Utah law violated the dormant Commerce Clause and the First Amendment).

[251] *See* FTC, Staff Report, Monitoring Software on Your PC: Spyware, Adware, and Other Software 3 (2005).

or installation to be adequate;[252] (2) questions regarding "whether the definition should limit 'spyware' to software that monitors and collects data relating to computer use";[253] and (3) "determining the nature and extent of harm that the software must cause."[254] Despite these questions, the FTC report provided a working definition of *spyware* as "software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge."[255]

Notwithstanding the lack of a uniform definition, certain types of software are commonly used as spyware. The Anti-Spyware Coalition (ASC) issued a report identifying examples of software that have been used to the detriment of computer users and thus could, under the right circumstances, qualify as spyware. These include:

1. advertising display software ("adware");
2. automatic download software ("tricklers");
3. dialing software ("unauthorized dialers");
4. passive tracking technologies ("unauthorized tracking cookies");
5. remote control software ("backdoors," "botnets," or "dronewear");
6. security analysis software ("hacker tools," "port and vulnerability scanners," or "password crackers");
7. system-modifying software ("hijackers" or "rootkits"); and
8. tracking software ("spyware," "snoopware," "unauthorized keylogger," or "unauthorized screen scraper").[256]

---

[252] *Id.* (noting that most but not all definitions include downloading or installation without consent).

[253] *Id.* (noting that such a definition "would not include software that does not collect data but adversely affects computer performance or otherwise interferes with the use of computers").

[254] *Id.* (finding agreement that spyware by definition should cause some harm to users but disagreement on the type and magnitude of the required harm).

[255] FTC, Staff Report, Monitoring Software on Your PC: Spyware, Adware, and Other Software at 1.

[256] Anti-Spyware Coalition, Working Report: Definitions and Supporting Documents (2005). This report provides descriptions of the positive and negative uses of the programs.

[2] Legal Requirements

Numerous state laws regulate spyware. These laws are summarized in the chart entitled "Selected State Anti-Spyware Laws," found in Appendix E. Below is a description of various federal enforcement mechanisms and an overview of several prominent state spyware laws.

[a] Federal Enforcement

There is no comprehensive federal law specifically designed to counter the threat of spyware. Both the FTC and Department of Justice (DOJ), however, have statutory authority to penalize certain types of malicious spyware distribution. Section 5 of the FTC Act prohibits the use of unfair or deceptive practices and empowers the FTC to prevent such practices.[257] The FTC uses this authority to bring enforcement actions and lawsuits against spyware distributors whose activities it believes to be in violation of section 5 of the FTC Act.[258] For example, the FTC has brought actions to challenge such activities as hijacking modems to place unauthorized telephone calls, hijacking Web pages or "copy catting" Web site domain names to subject consumers to an onslaught of pop-up ads, and sending spam to consumers through the use of information obtained when the consumers purchased an anti-spam product.[259]

---

[257] 15 U.S.C.A §§ 41–58 (West 2007). *See* discussion of FTC's enforcement authority in Chapter 16.

[258] *See, e.g.*, FTC v. Enternet Media, Inc., No. CV05-7777CAS (AJWx) (C.D. Cal. filed Dec. 11, 2006); FTC v. Seismic Entm't Prods., Inc., No. 1:04-CV-00377-JD (D.N.H. filed Oct. 30, 2006). *See also* FTC, Enforcement Actions, http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm (last visited June 30, 2009) (listing cases).

[259] FTC, Staff Report, *supra* note 251, at 20 (citing *In re* Bonzi Software, Inc., FTC Dkt. No. C-4126 (Oct. 6, 2004); FTC v. BTV Indus., Inc., Civ. Act. No. CV-S-02-0437-LRH-PAL (D. Nev. Feb. 11, 2004); FTC v. Baith, Civ. Act. No. CV S-03-1306-LRH-RJJ (D. Nev. Feb. 11, 2004); FTC v. D-Squared Solutions, LLC, Civ. Act. No. AMD 03-CV310 (D. Md. Nov. 6, 2003); FTC v. Alyon Techs., Inc., Civ. Act. No. 1: 03-CV-1297 (N.D. Ga. May 15, 2003); FTC v. Verity Int'l Ltd., Civ. Act. No. 00-Civ. 7422 (LAK) (S.D.N.Y. Nov. 21, 2002); FTC v. NetSource One, Civ. Act. No. 022-3077 (W.D. Ky. Nov. 2, 2002); FTC v. John Zuccarini, Civ. Act. No. 01-CV-4854 (E.D. Pa. May 24, 2002); FTC v. RJB Telecom, Inc., Civ. Act. No. 00201-7 (Phx) (D. Ariz. Sept. 26, 2001); FTC v. Hillary Sheinkin, Civ. Act. No. 2-00-3636-18 (D.S.C. Aug. 29, 2001); FTC v. Ty Anderson, Civ. Act. No. C00-1843P (W.D. Wash. Aug. 29, 2001); FTC v. Carlos Pereira, Civ. Act. No. 99-1367-A (N.D. Va. Feb. 12, 2001); FTC v. Audiotext Commc'ns, Civ. Act. No. Cv-97 0726 (DRH) (E.D.N.Y. Nov. 4, 1997); *In re* Beylen Telecom, Ltd., 125 F.T.C. 276 (1998)).

DOJ also has the authority, pursuant to a variety of statutes, to prosecute spyware distributors who compromise consumers' privacy or security or who obtain information fraudulently.[260] For example, the Computer Fraud and Abuse Act[261] (CFAA) criminalizes the following actions, among others: (1) compromising the confidentiality of a computer; (2) accessing a computer to defraud and obtain value; (3) knowing transmission and intentionally causing damage; (4) intentional access and thereby recklessly causing damage; and (5) trafficking in passwords.[262] DOJ regularly uses the CFAA to prosecute distributors of spyware.[263]

[b] State Enforcement

To date, more than 15 states have enacted laws restricting the use of spyware.[264] California's Consumer Protection Against Computer Spyware Act (CPACSA) was adopted in 2004[265] and is similar to several other states' anti-spyware statutes adopted thereafter.

The CPACSA forbids unauthorized users willfully, knowingly, or with ''conscious avoidance of actual knowledge'' to cause computer software to be copied onto a California consumer's computer and to use

---

[260] FTC, Staff Report, *supra* note 251, at 21.

[261] 18 U.S.C.A § 1030 (West 2007 & Supp. 2009). *See also* section 9.09[C].

[262] 18 U.S.C.A. § 1030; *see also* Computer Crime & Intellectual Prop. Section, United States Dep't of Justice, Prosecuting Computer Crimes 2 (Scott Eltringham ed., 2007), *available at* http://www.usdoj.gov/criminal/cybercrime/ccmanual/index.html.

[263] *See* Computer Crime & Intellectual Prop. Section, United States Dep't of Justice, Computer Crime Cases, http://www.usdoj.gov/criminal/cybercrime/cccases.html (last visited June 30, 2009).

[264] *See, e.g.*, Alaska Stat. §§ 45.45.792–45.45.798 (LEXIS 2008); Ariz. Rev. Stat. Ann. §§ 44-7301 to 44-7304 (West, Westlaw 2009); Ark. Code Ann. §§ 4-111-101 to 4-111-105 (LEXIS 2009); Cal. Bus. & Prof. Code §§ 22,947–22,947.6 (West, Westlaw 2009); Ga. Code Ann. §§ 16-9-150 to 16-9-157 (LEXIS 2009); 720 Ill. Comp. Stat. Ann. 5/16D-1 to 5/16D-7 (LEXIS 2009); Ind. Code Ann. § 24-4.8 (Burns, LEXIS 2009); Iowa Code Ann. § 715 (West, Westlaw 2009); La. Rev. Stat. Ann. §§ 51:2006–51:2014 (West, Westlaw 2008); Nev. Rev. Stat. Ann. §§ 205.473–205.513 (LEXIS 2009); N.H. Rev. Stat. Ann. § 359-H (West, Westlaw 2009); N.Y. Penal Law § 156 (McKinney, Westlaw 2009); R.I. Gen. Laws § 11-52 (LEXIS 2008); Tex. Bus. & Com. Code Ann. § 324 (Vernon, Westlaw 2009); Utah Code Ann. §§ 13-40-101 to 13-40-401 (LEXIS 2009); Va. Code Ann. §§ 18.2-152.1, 18.2-152.2, 18.2-152.4 (LEXIS 2009); Wash. Rev. Code Ann. § 19.270 (LEXIS 2009). For more details regarding these statutes, see Appendix E. In addition, Hawaii's computer crime law also contains limited spyware provisions. *See* Haw. Rev. Stat. Ann. §§ 708-890 to 708-895.7 (Michie, LEXIS 2009).

[265] Cal. Bus. & Prof. Code § 22947–22947.6 (West, Westlaw 2009).

such software, through intentionally deceptive means, to do any of the following:

1. modify certain Internet settings of an authorized user;
2. collect personally identifiable information under specified circumstances;
3. prevent an authorized user from blocking or disabling software through automatic reinstallation or reactivation;
4. intentionally misrepresent that an authorized user can uninstall or disable software through a particular action; or
5. remove or disable security, anti-spyware, or antivirus software.[266]

A different provision of the CPACSA forbids unauthorized users willfully, knowingly, or with "conscious avoidance of actual knowledge" to cause computer software to be copied onto a California consumer's computer and to use the software to do any of the following:

1. take control of the computer by transmitting commercial e-mail or a computer virus without authorization, using an Internet connection to damage the computer or to cause an authorized user to incur financial charges for a service he did not authorize, using the consumer's computer as part of a computer network for the purpose of damaging another computer, or "opening multiple, sequential, stand-alone advertisements" in the Internet browser without authorization and "with knowledge that a reasonable computer user cannot close the advertisements without turning off the computer or closing the . . . browser";
2. modify any of the authorized user's Internet security settings for the purpose of damaging one or more computers or, where such settings are intended to protect information, for the purpose of stealing personal information about the authorized user; or
3. prevent, without authorization, an authorized user's reasonable efforts to block or disable software by presenting a false option to decline installation where selecting such action does not actually

[266] Cal. Bus. & Prof. Code § 22947.2.

prevent the installation or by falsely representing that the software has been disabled.[267]

More broadly, the CPACSA prohibits any unauthorized user from installing software onto a California consumer's computer by intentionally misrepresenting that the software is necessary for security or privacy or to access or display certain content. The law also prohibits deceptively causing software to be introduced to a computer with the intent of causing an authorized user to use the software in a way that violates the statute.[268] The CPACSA lacks a provision specifically prescribing the means through which it is enforced or the penalties resulting from a violation, but it is likely enforceable against persons and entities as an act of unfair competition under California's Unfair Competition Law.[269]

Several other states have adopted anti-spyware statutes that resemble the CPACSA. Most of these statutes, however, contain enforcement or penalty provisions. The enforcement and penalty provisions vary widely from state to state, and include public and private enforcement, monetary fines, and criminal penalties.[270]

A handful of states have laws providing more limited protections. For example, Alaska's anti-spyware law does not contain the general prohibitions that many other state laws contain on the use of spyware for unauthorized access, modification, acquisition of data, or unauthorized control or use of a computer. Instead, the Alaska law prohibits unauthorized users from causing a pop-up advertisement to appear by means of a spyware program, knowing that the pop-up advertisement is (1) displayed

---

[267] Cal. Bus. & Prof. Code § 22947.3.

[268] Cal. Bus. & Prof. Code § 22947.4.

[269] *See* Cal. Bus. & Prof. Code §§ 17200–17,210.

[270] *See, e.g.*, Ariz. Rev. Stat. Ann. § 44-7304 (West, Westlaw 2009); Ark. Code Ann. § 4-111-104 (LEXIS 2009); Ga. Code Ann. § 16-9-155 (LEXIS 2009); 720 Ill. Comp. Stat. Ann. 5/16D-3(b), 5/16D-4(b), 5/16D-5(b), 5/16D-6 (LEXIS 2009); Ind. Code Ann. §§ 24-4.8-3-1 to 24-4.8-3-2 (Burns, LEXIS 2009); Iowa Code Ann. §§ 715.7–715.8 (West, Westlaw 2009); La. Rev. Stat. Ann. §§ 51:2012–51:2014 (West, Westlaw 2008); Nev. Rev. Stat. Ann. §§ 205.473–205.513 (LEXIS 2009); N.H. Rev. Stat. Ann. §§ 359-H:3 to 359-H:4 (West, Westlaw 2009); N.Y. Penal Law §§ 156.05–156.35 (McKinney, Westlaw 2009); R.I. Gen. Laws §§ 11-52-5 to 11-52-6, 11-52.2-6 (LEXIS 2008); Tex. Bus. & Com. Code Ann. §§ 324.101–324.102 (Vernon, Westlaw 2009); Va. Code Ann. §§ 18.2–152.12 (LEXIS 2009); Wash. Rev. Code Ann. § 19.270.060 (LEXIS 2009). Hawaii's computer crime law contains provisions relating to spyware that are categorically similar to those in CPACSA but are more limited in scope. For more information regarding these statutes, see Appendix E.

in response to a user's accessing a specific registered trademark, registered service mark, registered domain name, or Web site; and (2) purchased or acquired by a person other than the mark owner, licensee, authorized agent, authorized user, or person advertising the lawful sale, lease, or transfer of products bearing the mark through a secondary marketplace.[271] It also prohibits purchasing advertising that violates the standard set forth above if the purchaser of the advertising "receives notice of the violation from the mark owner" and "fails to stop the violation."[272] While these provisions are strict with regard to pop-up advertisements specifically, they do not address the wider spectrum of potential spyware uses.

Utah's anti-spyware law also differs from the California model. Like Alaska's anti-spyware statute, Utah's Spyware Control Act[273] focuses exclusively on prohibiting pop-up advertisements. Specifically, the law prohibits persons from displaying a pop-up advertisement by means of spyware if the pop-up advertisement (1) is displayed in response to a specific registered trademark, registered service mark, registered domain name, or Web site address; (2) constitutes infringement of a registered trademark under federal or state law; and (3) is purchased or acquired by a person other than the mark owner or his authorized agent, licensee, authorized user, a "person advertising the lawful sale, lease, or transfer of products bearing the mark through a secondary marketplace," or a "person engaged in a fair or otherwise permissible use of a trademark or service mark under applicable trademark law."[274] Persons who violate Utah's Spyware Control Act are subject to injunctions and monetary penalties and may be sued by the Attorney General of Utah or privately by a mark owner who does business in Utah and is adversely affected by the violation.[275]

[I] ISO 27001 and 17799/27002

The International Organization for Standardization (ISO) is a non-governmental organization composed of the national standards institutes of 161 countries.[276] ISO sets international standards across a range of

[271] Alaska Stat. § 45.45.792 (LEXIS 2008).

[272] *Id.*

[273] Utah Code Ann. §§ 13-40-101 to 13-40-401 (LEXIS 2009).

[274] Utah Code Ann. § 13-40-201.

[275] Utah Code Ann. § 13-40-301.

[276] For more information about ISO, see International Organization for Standardization, International Standards for Business, Government and Society, http://www.iso.org/iso/home.htm (last visited Aug. 18, 2009).

industries. In the area of information security, ISO has promulgated two important standards: 27001 and 17799/27002.

ISO 27001 provides a "process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System."[277] It is a flexible standard, and users are encouraged to (1) understand their information security requirements and the need to establish policy objectives for information, (2) implement controls to manage information security risks in the context of the organization's overall business risks, (3) monitor and review the performance and effectiveness of the Information Security Management System, and (4) continually improve the Information Security Management System based on objective measurement.[278]

ISO 17799/27002 contains numerous best practice recommendations for information security controls and is intended to establish "guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization."[279] The standard contains:

> [B]est practices of control objectives and controls in the following areas of information security management:
>
> - security policy;
> - organization of information security;
> - asset management;
> - human resources security;
> - physical and environmental security;
> - communications and operations management;
> - access control;
> - information systems acquisition, development and maintenance;
> - information security incident management;
> - business continuity management; and
> - compliance.[280]

Specific controls are not considered mandatory because an organization seeking certification under the standard is expected to select specific

---

[277] ISO/IEC 27001:2005—Information technology—Security techniques—Information security management systems—Requirements (International Org. for Standardization & Int'l Electrotechnical Comm'n 2005).

[278] *Id.*

[279] ISO/IEC 17799:2005 FAQs, http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm (last visited Sept. 20, 2009).

[280] *Id.*

controls only after undertaking a security risk assessment.[281] For more information about ISO 27001 and 17799/27002, visit *http://www.iso.org*.

[J] Statement on Accounting Standards 70 Audits

Statement on Accounting Standards 70 is a widely recognized auditing standard established by the American Institute of Certified Public Accountants (AICPA) in 1992 to assess the adequacy of internal controls implemented by service providers that host or process data on behalf of others.[282] A SAS 70 audit of a service provider is often necessary for an independent auditor to assess the financial statements of an entity that obtains the services of the service provider because the service provider's controls may have an impact on the controls of the entity subject to the audit. In an effort to avoid duplicative SAS 70 audits on behalf of numerous customers, service providers often retain independent auditors to conduct their own SAS 70 audit, the results of which are shared with the service providers' customers and their auditors when requested.

There are two types of reports that may be generated by independent auditors as a result of a SAS 70 audit: Type I and Type II. At a high level, Type I reports describe the controls a service provider has in place as of a specific date.[283] Type II reports contain the same description but also include the results of detailed testing of the controls over a six-month period.[284]

SAS 70 reports are a useful tool for companies that retain service providers to establish compliance with the requirements of various information security laws. For example, GLB[285] and the Safeguards Rule implementing GLB require financial institutions to ensure that their third-party service providers are compliant with the rules set forth in GLB to the same extent as the financial institutions are themselves. A review of service providers' SAS 70 Type II reports are one way financial institutions that retain service providers can comply with this requirement. Similarly, the security standards promulgated as part of HIPAA[286] require

---

[281] *Id.*

[282] Codification of Accounting Standards and Procedures, Statement on Auditing Standards No. 70 (American Inst. of Certified Pub. Accountants 1992).

[283] *See* Codification of Accounting Standards and Procedures, Statement on Auditing Standards No. 70 ¶ 24.

[284] *See id.*

[285] For more information, see section 3.02.

[286] For more information, see section 4.02.

evaluation of information security processes and management of health plans, health care clearinghouses, and certain health care providers. Though the standards set forth in HIPAA are not coextensive with those of a SAS 70 Type II audit, SAS 70 Type II reports have become effective and useful components of HIPAA compliance programs for covered entities.

SAS 70 Type II reports also are useful for purposes of establishing compliance with SOX.[287] Outsourced functions may impact a company's financial reporting or internal controls. SOX section 404 requires management to take responsibility for, evaluate, and report on the company's internal controls over financial reporting.[288] This responsibility extends to outsourced operations to the extent they constitute part of the company's internal controls over financial reporting.[289] The Public Company Accounting Oversight Board (PCAOB) has adopted (and the SEC has approved[290]) standards describing when a third-party service organization's services are part of a company's information systems.[291] Under the SOX regime, management is thus responsible for evaluating certain controls over outsourced operations. Considering the obvious difficulties and costs involved in conducting such an evaluation, many companies find it preferable to rely on a SAS 70 report. The SEC has condoned the use of SAS 70 Type II reports in meeting the requirements of SOX section 404.[292]

[K] Payment Card Industry Data Security Standard

[1] Overview

The PCI DSS is a set of technical and business requirements for the processing of credit and debit card data.[293] American Express, Discover,

---

[287] For more information, see section 14.02[D].

[288] For more information, see section 14.02[D][2][a].

[289] SEC, Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports: Frequently Asked Questions (revised Sept. 24, 2007), *available at* http://www.sec.gov/info/accountants/controlfaq.htm#foot1 (Question 8) [hereinafter SEC, Internal Control FAQs].

[290] Pursuant to authority granted in 15 U.S.C.A. § 7217 (West 2007).

[291] *See* PCAOB Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements ¶ B18 (June 12, 2007).

[292] *See* SEC, Internal Control FAQs, *supra* note 289, Question 8 ("In assessing internal controls over financial reporting, management may rely on a Type 2 SAS 70 report performed by the auditors of the third party service providers.").

[293] PCI Sec. Standards Council, Payment Card Industry Data Security Standard (Ver. 1.2.1, July 2009), *available at* https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html (last visited Sept. 20, 2009). In addition to the PCI DSS itself, the

JCB, MasterCard, and Visa jointly developed the PCI DSS and created the PCI Security Standards Council to manage the Standard. The PCI DSS applies to all entities that process (e.g., collect, store, or transmit) credit or debit card data, such as merchants, service providers, acquirers, security assessors, and vendors.[294]

The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.[295] The Standard is intended to help organizations proactively protect customer payment card account data. Unlike many industry and government security standards that contain general principles, the PCI DSS sets forth specific requirements. The core of the PCI DSS is a group of principles and accompanying requirements. These requirements apply to all of a covered entity's network components (such as firewalls, switches, routers, wireless access points, network appliances, and other security appliances), servers (such as Web, application, database, authentication, mail, proxy, NTP (network time protocol), and DNS (domain name system) servers), and applications that contain cardholder data and sensitive authentication data.[296]

The PCI DSS prohibits the storage of sensitive authentication data, such as magnetic stripe data, payment card security code numbers, and debit card PIN authentication numbers after the card payment has been authorized.[297] Covered entities may retain certain cardholder data, such as the primary account number (PAN), cardholder name, card expiration date, and service code for business or legal compliance purposes.[298] Entities that process cardholder name, card expiration date, and service code in conjunction with the PAN must comply with the requirements of the Standard.[299] In addition, the PCI DSS recommends that covered entities

---

PCI Security Standards Council has published numerous PCI-related documents, including (1) a glossary of defined terms used in the PCI DSS, (2) a set of frequently asked questions about the PCI DSS, and (3) self-assessment questionnaires for qualifying merchants and service providers. All of these PCI-related documents are available at https://www.pcisecuritystandards.org.

[294] PCI Sec. Standards Council, Payment Card Industry Data Security Standard (Ver. 1.2.1, July 2009), *available at* https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html (last visited Sept. 20, 2009).

[295] *Id.*

[296] *Id.*

[297] *Id.*

[298] *Id.*

[299] *Id.*

isolate cardholder data from the remainder of the corporate network to reduce the scope and cost of PCI DSS assessments, the cost and difficulty of implementing and maintaining PCI DSS controls, and the risk associated with processing cardholder data.[300] The PCI DSS also recommends that covered entities develop a clear understanding of business requirements and processes that drive the need to process cardholder data and understand and document relevant data flows.[301]

[2] Requirements

The PCI DSS principles and requirements are as follows:

- *Requirement 1:* "Install and maintain a firewall configuration to protect cardholder data."[302] This requires that "all systems . . . be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources."[303]
- *Requirement 2:* "Do not use vendor-supplied defaults for system passwords and other security parameters."[304] The purpose of this requirement is to preclude individuals who may have access to vendor default passwords or other vendor default settings from compromising covered entities' systems.
- *Requirement 3:* "Protect stored cardholder data."[305] Covered entities are required to protect cardholder data using methods such as "encryption, truncation, masking and hashing. . . ."[306]
- *Requirement 4:* "Encrypt transmission of cardholder data across open, public networks."[307] This provision sets forth a specific requirement to

[300] *Id.*
[301] *Id.*
[302] *Id.*
[303] *Id.*
[304] *Id.*
[305] *Id.*
[306] *Id.*
[307] *Id.*

encrypt sensitive information "during transmission over networks that are easily accessed by malicious individuals."[308]

- *Requirement 5:* "Use and regularly update anti-virus software."[309] Covered entities must protect all systems commonly affected by malware (such as viruses, worms, and Trojans) from "current and evolving malicious software threats."[310]
- *Requirement 6:* "Develop and maintain secure systems and applications."[311] Covered entities must continuously update relevant systems with the latest vendor-supplied security patches.
- *Requirement 7:* "Restrict access to cardholder data by business need-to-know."[312] The provision requires covered entities to implement systems and processes to limit access to the smallest amount of cardholder data needed to fulfill relevant job responsibilities.
- *Requirement 8:* "Assign a unique ID to each person with computer access."[313] This requirement is designed to facilitate individual accountability for access to cardholder data.
- *Requirement 9:* "Restrict physical access to cardholder data."[314] This provision requires appropriate control of physical access to data or systems, which limits the opportunity for access to or removal of cardholder data.
- *Requirement 10:* "Track and monitor all access to network resources and cardholder data."[315] This requirement is intended to assist in determining the cause of a compromise of cardholder data and analyzing security incidents.
- *Requirement 11:* "Regularly test security systems and processes."[316] The frequent testing is designed to test the systems' ability to resist attacks from continuously evolving threats.

---

[308] *Id.*
[309] *Id.*
[310] *Id.*
[311] *Id.*
[312] *Id.*
[313] *Id.*
[314] *Id.*
[315] *Id.*
[316] *Id.*

- *Requirement 12:* "Maintain a policy that addresses information security for employees and contractors."[317] Covered entities should implement strong security policies to set expectations for their personnel.[318] Personnel should be appropriately trained on the covered entity's compliance programs and their roles and responsibilities in protecting cardholder data.[319]

[3] Compliance Validation

Each payment card brand has its own PCI DSS compliance validation program.[320] Entities subject to the PCI DSS are required to validate their compliance on an annual basis. The specific requirements necessary to certify compliance depend on the type of entity involved in the processing of payment cards and the number of payment cards processed by the covered entity pursuant to each payment card brand's compliance validation program.

For example, pursuant to MasterCard's Site Data Protection Program, there are four levels of merchants, and the compliance validation requirements imposed on a given merchant depend on the level the merchant is assigned. MasterCard assigns Level 1 status to any merchant that (1) has suffered a hack or an attack that resulted in an account data compromise, (2) has greater than six million total combined MasterCard and Maestro transactions annually, and (3) MasterCard determines should meet the Level 1 merchant requirements to minimize risk to the system.[321] All MasterCard Level 1 merchants are required to complete an annual onsite assessment conducted by a certified Qualified Security Assessor and conduct quarterly network scans using an Approved Scanning Vendor.[322] Similarly, American Express has three merchants levels and

---

[317] *Id.*

[318] *Id.*

[319] *Id.*

[320] *See, e.g.*, MasterCard Worldwide, The MasterCard SDP Program (Site Data Protection), http://www.mastercard.com/us/sdp/index.html (last visited Sept. 19, 2009); Visa, Cardholder Information Security Program, http://www.visa.com/cisp (last visited Sept. 19, 2009); American Express, American Express Data Security Operating Policy for U.S. Merchants, https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US.pdf (last visited Sept. 19, 2009).

[321] MasterCard Worldwide, The MasterCard SDP Program (Site Data Protection), http://www.mastercard.com/us/sdp/index.html (last visited Sept. 20, 2009).

[322] *Id.*

assigns Level 1 status to any merchant that (1) has greater than 2.5 million American Express Card transactions per year; (2) has had a data incident; or (3) American Express otherwise deems a Level 1 merchant. All American Express Level 1 merchants are required to complete an annual onsite security assessment and to conduct quarterly network scans.[323]

In addition to merchants, all service providers that store, process, or transmit payment card transactions must comply with the PCI DSS. As with merchants, each payment card brand has its own compliance validation requirements for service providers.[324] The payment card brands also maintain a list of service providers in compliance with the PCI DSS, and all entities subject to the PCI DSS are required to use PCI DSS–compliant service providers.[325]

Covered entities that fail to comply with the PCI DSS face fines and increases in the rates the card brands charge for each transaction.[326] Non-compliant entities also may be denied the ability to accept payment cards. Where non-compliance with the PCI DSS results in a breach of payment card data, the affected card brand may impose a fine of as much as $500,000 per incident and require payment of costs associated with the breach.[327]

---

[323] American Express, American Express Data Security Operating Policy for U.S. Merchants, https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US.pdf (last visited Sept. 19, 2009).

[324] *See, e.g.*, MasterCard Worldwide, The MasterCard SDP Program (Site Data Protection), http://www.mastercard.com/us/sdp/index.html (last visited Sept. 19, 2009); Visa, Cardholder Information Security Program, http://www.visa.com/cisp (last visited Sept. 19, 2009); American Express, American Express Data Security Operating Policy for U.S. Merchants, https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US.pdf (last visited Sept. 19, 2009).

[325] *See, e.g.*, Visa, Cardholder Information Security Program, http://www.visa.com/cisp (last visited Sept. 19, 2009) (stating that "issuers and acquirers must use, and are responsible for ensuring that their merchants use, service providers that are compliant with the [PCI DSS]. Although there may not be a direct contractual relationship between merchant service providers and acquirers, Visa issuers and acquirers are responsible for any liability that may occur as a result of non-compliance." Visa, Cardholder Information Security Program: Service Providers, http://usa.visa.com/merchants/risk_management/cisp_service_providers.html (last visited Sept. 19, 2009)).

[326] PCI Compliance 26 (Tony Bradley ed., Syngress Publ'g, Inc., 2007).

[327] Visa, Cardholder Information Security Program: If Compromised, http://www.visa.com/cisp (last visited Sept. 19, 2009).

[L] Developing an Information Security Program[328]

[1] Overview

The development of a written information security program has become a de facto requirement for organizations that maintain personal information. Having such a program in place is a legal requirement for many entities (such as financial institutions). The myriad information security laws and standards in effect impose a series of obligations on organizations that collect and maintain personal information. A written information security program provides a comprehensive means to organize compliance with applicable requirements. Although organizations' information security needs differ depending on the organizations' size and complexity, the nature and scope of their activities, and the sensitivity of the personal information they collect and maintain, there are certain core concepts that should be incorporated into every information security program.

[2] Assessing the Risk

The development of an information security program should begin with a comprehensive understanding of the types of personal information the organization collects and maintains. The first step in crafting an effective program is to conduct an inventory of the entity's personal information data flows. The focus of such an inventory should be personal information of both consumers and employees that is maintained by the organization. Preparing an inventory of data flows often is accomplished in the context of a larger privacy and information security assessment. This assessment should begin with a series of questions:

1. What personal information does the entity collect? For purposes of the initial inquiry, personal information should be defined broadly to include name, postal address, e-mail address, telephone number, date of birth, Social Security number, driver's license number, account number, credit or debit card information, and health or medical information.

[328] This section is derived from the chapter entitled "Developing an Information Security Program," published by the ABA in its Data Security Handbook. *See* American Bar Association, Data Security Handbook 107 (American Bar Association 2008).

2. How is each category of personal information used? There are often multiple uses for individual sets of data.
3. Where is the personal information stored? Data may be stored in multiple media. Each storage media should be cataloged.
4. To whom is the personal information disclosed? Consider both internal and external disclosures.
5. Who has access to the personal information and for what purpose? Numerous parties may have authorized access to the data. For example, in addition to employees who need to see the data to perform their jobs, are there consultants or third-party service providers that need access to the information to carry out their obligations to the entity?
6. How is the personal information ultimately disposed of? Consider disposal practices with respect to each medium in which personal information is maintained. For example, a particular set of customer data may be maintained in an electronic database. The data set may be printed from time to time (thus creating a hard copy of the personal information), and the database may also be backed up (resulting in backup tapes containing the information) or saved onto portable media devices (resulting in other media containing the information).

To answer these questions most effectively, it is necessary to identify the relevant employees and third parties who have knowledge of the organization's personal information data flows. These individuals can pinpoint which data flows to consider in conducting a privacy assessment, thus cataloging the information sets that will be evaluated further. It is often useful to begin with the human resources, marketing, and information technology departments. Other departments to consider include sales, research and development, and legislative affairs. These typically are the components of an organization that collect and use significant amounts of personal information.

Once the key individuals are identified, the data inventory process can begin by having the relevant individuals complete a questionnaire that requests information about data collection and use practices within their department. A written questionnaire is a useful starting point, but it also will be necessary to conduct face-to-face interviews. In-person meetings ultimately provide the most successful forum in which to elicit accurate

information about a company's data flows. Keep in mind that the interview process may be a lengthy one, depending on the resources that can be devoted to the project.

After the interviews have been conducted, data flow maps can be prepared to visually depict the flow of personal information throughout the organization. Data flow maps provide a snapshot of the entity's current uses of personal information. They also can provide an ongoing management tool.

After gaining an understanding of the organization's data flows, the next step is to identify and assess the risk of compromise to the personal information at each stage in the information flow, from initial collection through ultimate disposition. While hacking incidents are the most obvious form of data compromise, there are many other significant forms of compromise to consider, including intentional or unintentional data misuse by employees, service providers, or business partners, and loss or theft of company equipment that contains personal information. It is critical to understand that the risk of compromise to personal information goes well beyond those risks associated solely with computer breaches and often results from vulnerabilities in business processes.

It is necessary to identify and assess information security risks within an organization from a holistic perspective. Thus, the team of individuals recruited to assist with the assessment should include business personnel, information technology experts, and legal and compliance personnel. Each group brings a different perspective to the project. Together, a diverse group of individuals can provide a thorough view of the entity's personal information practices. In this way, the entity will be able to most effectively identify information security vulnerabilities and minimize the possible impact of threats to the security of the information.

Based on the results of the risk assessment, the next step is to determine whether there are any areas in which existing information practices may be exacerbating risks to the security of the personal information. If existing safeguards are not adequate, it will be necessary to make changes going forward. The likelihood that a given risk will occur and the severity of the consequences if it does should inform the prioritization of any changes to be made. The effectiveness of the available security measures and their cost relative to the harm caused by an information security breakdown should also be considered.

After the assessment process has been completed, the organization can consider the core concepts that will form the backbone of the entity's

information security program. These basic concepts must include, at a minimum, (1) administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of the personal information maintained by the organization; (2) managerial coordination and accountability; (3) guidance with respect to the use of third parties that access the entity's personal information; and (4) a systematic approach to identifying and responding to security incidents involving personal information maintained by the entity. In developing a comprehensive information security program, it is essential that the program not simply be embodied in a document that will be unread and unheeded by employees. The program, once developed, must be made part of the organizational ethos so that information security becomes second nature to all relevant employees.

[3] Administrative, Technical, and Physical Safeguards

Every information security program must contain administrative, technical, and physical safeguards intended to protect the personal information that is entrusted to the organization, whether the data are maintained internally or stored by a third-party service provider. Each category of data security is discussed in turn below.

[a] Administrative Safeguards

In many ways, developing a series of technical and physical security requirements that are appropriate to the organization and documenting them in an information security policy are the straightforward aspects of crafting an effective information security program. The more challenging task is to administer these security measures so they are implemented effectively by the organization.

The most important administrative security measure is to create employee awareness around the importance of information security. Without meaningful consideration by employees, an information security program is worthless. At the commencement of the program, employees must be trained and regularly reminded of the entity's requirements to protect personal information (including the physical and technical security rules that have been implemented by the organization). The information security program also must include disciplinary measures for information

security violations by employees. Other administrative safeguards to consider include:

1. appointing an individual within the organization who is ultimately responsible for information security and accountable for the successful implementation and maintenance of the program;
2. conducting background checks, with a focus on past instances of fraud, before hiring employees who will have access to personal information (and conducting periodic screening of current employees who have regular access to sensitive personal information);
3. having employees sign a privacy and information security agreement that explains the organization's expectations regarding the appropriate handling of personal information;
4. developing detailed contingency plans in the event of an emergency or other similar occurrence that damages the systems in which personal information is stored—these plans should contemplate, at a minimum, the (a) maintenance of retrievable copies of electronic personal information, (b) restoration of any lost data, and (c) protection of the security of electronic personal information while operating in an emergency mode; and
5. implementing an extensive audit program to monitor compliance with the organization's information security program.

[b] Technical Safeguards

As it is with physical security, an essential aspect of technical security is access control. In the context of technical security, this means role-based controls on access to workstations and other electronic media containing personal information. Only those individuals who have been granted specific access rights should be permitted access to personal information housed on systems owned by the organization. Role-based access controls at the workstation level are administered by the provision of user IDs and strong passwords to track the identities of users. The organization's information security policy should contain a requirement that these user IDs and passwords be unique and reset at least every three months or more frequently as circumstances require (e.g., when an employee is

transferred to a new position or separated from the organization). From a user authentication perspective, any user who has failed to enter the correct user ID and password after a designated number of log-on attempts should be prohibited from accessing the workstation without the specific approval of a supervisor. In addition to these role-based access controls, organizations should consider including within their information security policies provisions that require:

1. immediate deactivation of terminated employees' user IDs and passwords;
2. automatic logoff on workstations after a predetermined time of inactivity (and training to activate a screensaver if leaving a workstation for a period of time);
3. encryption of electronic files containing personal information;
4. technical security requirements to guard against unauthorized access to electronic personal information that is being transmitted over an electronic communications network;
5. use of secure socket layer or other secure connection when personal information is transmitted over the Internet;
6. audit controls that record and examine activity in information systems that contain or use electronic personal information;
7. technical requirements to protect electronic personal information from improper alteration or destruction, including mechanisms to ensure that electronic personal information has not been altered or destroyed in an unauthorized manner; and
8. verification requirements to authenticate a person or entity seeking access to electronic personal information.

[c] Physical Safeguards

At its most basic level, physical security means limiting access to the hardware and other media that contain personal information. To limit access to data, access controls should be put in place at the facility level, the workroom level, and the workstation level based on the roles of individuals within the organization. The same individual who has unfettered access to the facility at large may not require access to the specific area within the facility in which workstations and other media containing

personal information are housed. Likewise, the employee who is given access to the areas of the facility in which the workstations are located may not require access to the workstations themselves. Effective role-based access controls should correspond to the information individuals need to carry out their job responsibilities.

In addition to limiting access to personal information based on roles within the workplace, other physical security requirements that should be considered are:

1. use of locked rooms and file cabinets for records containing personal information;
2. close scrutiny of the hardware and other media that contain personal information, including an accurate inventory of such equipment or media and their movement within, and outside, the facility;
3. appropriate disposal standards for records containing personal information and hardware or other media on which it is stored, which generally means requiring that the information or media be recycled, shredded, or otherwise destroyed such that the information is rendered unreadable; this can be accomplished by requiring that hard-copy records containing personal information be burned, pulverized, or shredded, and that computers and other electronic media containing personal information be destroyed or the data permanently deleted;
4. removal of personal information from hardware or media before the hardware or media are made available for reuse within the organization;
5. protection of records containing personal information against damage or destruction arising from physical hazards such as fire or flood;
6. use of security guards and surveillance cameras to monitor areas of the company where sensitive personal information is stored; and
7. authorization of visitors before entering areas where personal information is stored. Visitors should be given a badge that identifies them as non-employees, which must be surrendered prior to leaving the facility.

[4] Responsibility for the Information Security Program

Whether an organization chooses to task a single employee with the responsibility of coordinating and maintaining the entity's information security program or disperses the responsibility among a team of employees, someone in the organization must be accountable for information security. In determining who should be charged with this responsibility, it should be recognized that, fundamentally, information security is a management issue, not a technology issue. Although information technology plays a significant role in protecting data, effective information security at the organizational level requires a broader focus. Even with respect to information technology, organizations must focus on managing the technology and not solely on the technology itself.

In addition, a successful information security program requires the coordination of multiple business units, including legal, human resources, information technology, audit, and business functions. The person or team that is chosen to coordinate the information security program must have the ability to communicate and work effectively with all of these different groups.

[5] Service Providers

Service provider and other third-party relationships pose significant information security risks for organizations that maintain personal information. When contracting with third parties that will have access to an organization's personal information, it is imperative to impose stringent contractual protections that will govern the privacy, confidentiality, and security of the personal information at issue. Although many organizations have traditional non-disclosure provisions in their third-party contracts, these provisions are not sufficient to protect the organization's interest in personal information. Traditional non-disclosure agreements typically seek to protect proprietary business information and thus do not address the myriad privacy and information security requirements that should be imposed on service providers with access to an organization's personal information.

Responsibility for legal compliance (and related reputational risk) ultimately rests with the disclosing organization. That is the entity to which individuals entrusted their information in the first place. Because the organization also must ensure that it complies with any privacy or information security representations it has made, it is important that the

entity establish a formal vendor qualification program that includes a checklist of items to consider prior to formalizing any vendor relationship. This checklist of due diligence items should, at a minimum, contain the following questions:

1. Does the vendor have information security policies and procedures in place? If so, a review of these policies and procedures is essential. Any vendor in the business of processing personal information on behalf of its customers should have an established, written information security program. A red flag should be raised if the vendor does not have such a program in place.
2. Does the vendor have the ability to segregate personal information it receives from each of its customers?
3. Does the vendor conduct regular training of its employees regarding maintaining the security, confidentiality, and integrity of personal information it receives from customers?
4. Have the vendor's information security practices been audited by an independent third party? If so, when and by whom? If available, a review of the audit can be instrumental.
5. Is the vendor certified by a recognized trade association or similar authority?
6. What is the vendor's objective reputation for handling personal information? If possible, seek information about the vendor and its information security practices from several references or other reliable sources.

Once an organization has reached a comfort level as a result of its due diligence efforts, the parties should enter into an agreement containing specific privacy, confidentiality, and information security provisions. In addition to an expansive definition of "personal information" that takes into account the myriad privacy and information security laws and outlines the scope of the information to be covered by the agreement, the relevant provisions should contain, at a minimum, all of the following covenants by the vendor:

1. Personal information provided by the disclosing party will be held in strict confidence by the vendor and its employees, agents, and subcontractors.

2. Personal information received by the vendor will be processed only for the purpose of performing services for or on behalf of the disclosing organization.
3. The vendor will comply with international, federal, state, and local privacy and data security laws and regulations, as well as applicable industry standards and the disclosing organization's own privacy and information security representations to individuals.
4. The vendor has obtained all authorizations that are required to lawfully perform the relevant services on behalf of the disclosing organization.
5. The vendor will not share the personal information it receives pursuant to the agreement with any third party unless specifically agreed to by the disclosing organization.
6. The vendor will conduct appropriate and periodic training of its employees with access to the disclosing party's personal information.
7. The vendor will conduct appropriate background screening of its employees who will have access to the disclosing party's personal information.
8. The vendor will maintain and implement a comprehensive, written information security program that includes appropriate administrative, technical, and physical safeguards to protect the personal information disclosed to the vendor.
9. The vendor will notify the disclosing organization immediately in the event of a breach of its obligations under the agreement or any security breach involving personal information provided by the disclosing organization.
10. The vendor will allow the disclosing organization to audit, monitor, and inspect the vendor's facilities, systems, and records for compliance with the agreement.
11. The vendor will return or render unreadable all of the personal information provided to it by the disclosing organization promptly when the agreement expires or is terminated.

Embedding these types of provisions into an agreement with a vendor that will access an organization's personal information will help

ensure that the information is not misused in the hands of the vendor. In addition to these types of provisions, an indemnity for breach of these clauses will provide additional contractual recourse to the disclosing organization. Of course, the creditworthiness of the vendor is operative in considering the real value of an indemnity.

While conducting due diligence and entering into an airtight privacy, confidentiality, and information security agreement are imperative, they are not sufficient on their own when sharing personal information with third parties. In addition, the organization providing access to personal information to a third party must conduct ongoing monitoring to ensure that the vendor is complying with its contractual obligations and continues to show appropriate care for the security of the personal information. Such monitoring may include site visits and periodic assessments of the third party's conduct.

[6] Incident Response Plan

Since 2003, when California first enacted its law requiring organizations to notify affected state residents of an information security breach, more than 45 other states, as well as Congress, have enacted similar breach notification laws.[329] As discussed in more detail in Chapter 15, the duty to notify individuals affected by a data security breach generally arises under breach notification laws when there is a reasonable belief that unencrypted, computerized personal information has been acquired or accessed by an unauthorized person.

While no information security is perfect, proactive incident response planning can help minimize the impact of a security breach. As described earlier, such planning includes inventorying databases that contain personal information, understanding how sensitive personal information flows throughout the organization, conducting ongoing risk assessments for internal and external risks to the data, responding to reasonably foreseeable risks, and maintaining a comprehensive written information security program. In addition, an incident response plan should be part of an overarching information security program.

---

[329] *See* Cal. Civ. Code § 1798.82 (West, Westlaw 2009); *see also* Chapter 15 and Appendix A.

An incident response plan should, at a minimum, cover the following topics:

1. *The Investigation*

If a possible security breach has occurred, the first step is to determine as quickly as possible whether the event triggers breach notification requirements that would require the organization to notify affected individuals of the incident. To make this determination, the organization will need to initiate an investigation of the incident.[330]

2. *Notification*

Once the extent and scope of the incident have been defined and it is determined that notification is required, the next step outlined in the incident response plan is notification of the affected individuals.

3. *Modification of Existing Business Practices*

Although information security requires constant vigilance, and businesses should evaluate and adjust their information security programs at regular intervals, an information security breach has the potential to provide businesses a good opportunity to revisit their existing practices and to make appropriate changes. A breach resulting in minimal harm can even offer a silver lining to organizations by providing the impetus to revisit those existing practices. A breach also serves to incentivize senior management to focus on information security and help ensure that appropriate human and financial resources are made available to strengthen information systems. Although no data security program is foolproof, gaining an understanding of new and emerging threats to information security and changes in the legal and regulatory environment can help mitigate risk associated with information security incidents.

[330] For more information, see section 15.03[A][1].