Richmond Journal of Law and Technology

Volume 21 | Issue 1 Article 3

2014

The Reasonable Information Security Program

Peter Sloan

THE REASONABLE INFORMATION SECURITY PROGRAM

Peter Sloan*

Cite as: Peter Sloan, *The Reasonable Information Security Program*, 21 RICH. J.L. & TECH. 2 (2014), http://jolt.richmond.edu/v21i1/article2.pdf.

I. INTRODUCTION

[1] Our information inhabits a perilous world. Cyber theft, cyber extortion, mobile device loss, misappropriation of confidential business information, and unauthorized disclosures of protected information are real and present dangers for organizations of all sizes and across all industries.[1]

* Peter Sloan is a partner at the law firm Husch Blackwell LLP and a founding member of the firm's Information Governance Group. For over a decade he had focused his law practice on how organizations can best retain, protect, preserve, and compliantly dispose of their records and information. He is an ARMA International member and a participant in Working Groups 1 and 11 of The Sedona Conference. He presents and writes frequently on information governance topics, including *The Compliance Case for Information Governance*, 20 RICH. J.L. & TECH. 4 (2014). The author thanks the JOLT staff for their patience and diligence; Cordero Delgadillo and Suzie Specker for their indefatigable research of FTC enforcement matters; and Kerri Steffens for her invaluable work in confirming the citations in this article. The views expressed, and any errors made, are solely those of the author, and such views are not attributable to his law firm or its clients.

[1] The Verizon 2014 Data Breach Investigations Report analyzed 1,367 security incidents that occurred during 2013 with confirmed data losses. *See 2014 Data Breach Investigations Report*, VERIZON 2 (2014), *available at* http://www.verizonenterprise.com/DBIR/2014/, *archived at* http://perma.cc/W9QD-SR28. Industries suffering such security incidents included: Finance, Public, Retail, Accommodation, Utilities, Professional, Manufacturing, Information, Education, Mining, Transportation, Administrative, Healthcare, Entertainment, Real Estate, Trade, Construction, and Management. *Id*. at 6. According to Verizon, the nine incident patterns that account for virtually all of these security incidents are: Web App Attacks (35%), Cyber-espionage (22%), Point-of-Sale Intrusions (14%), Card Skimmers (9%), Insider Misuse (8%), Crimeware (4%), Miscellaneous Errors (2%), Physical Theft/Loss

[2] Organizations must also navigate a bewildering landscape of data security fiefdoms within United States' federal and state law, under which specific types of entities must safeguard specific kinds of protected information.[2] Moreover, the Federal Trade Commission ("FTC") has enforced data security in numerous matters without underlying regulatory standards, employing the legal theory that inadequate information security is an unfair business practice.[3]

[3] The reality is that security breaches may be inevitable no matter how diligently an organization safeguards its information. As then FBI Director, Robert Mueller, observed in 2012, "[t]here are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again."[4] Perhaps in recognition that security perfection is unattainable, information security laws share a common theme of reasonableness. The notion of reasonableness permeates explicit statutory and regulatory requirements for safeguarding information, and appears to be a central tenet of FTC enforcement orders regarding information security. Yet such legal requirements and orders frequently fail to specify what reasonableness means in their particular domains. And so, one is left to wonder, what constitutes a "reasonable" information security program?

[4] Section II of this article explores the pertinence of reasonableness in different expressions of United States' information security law, from the protection of trade secrets to prescriptive data security requirements

(< 1%), and Denial of Service Attacks (0%, due to cohort requirement of confirmed data loss). *Id.* at 14.

[2] *See infra* Part II.B.

[3] *See infra* Part II.D.

[4] Stacy Cowley, *FBI Director: Cybercrime will eclipse terrorism*, CNN (Mar. 2, 2012, 7:55 AM), http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/, *archived at* http://perma.cc/7J3L-Q8XX.

under HIPAA, Gramm-Leach-Bliley, FACTA, COPPA, and the wide range of state laws mandating safeguards for protected information, as well as the U.S.-EU Safe Harbor Privacy Principles, and ultimately FTC enforcement proceedings under Section 5 of the FTC Act.

[5] Section III proposes six essential elements of a reasonable information security program, derived from United States' federal and state legal requirements, as well as voluntary standards—including ISO 27002 [5] and the Framework for Improving Critical Infrastructure Cybersecurity recently published by the National Institute of Standards and Technology ("NIST"). [6] As discussed more fully in Section III, a

[5] ISO 27002 is an international, voluntary standard, the code of practice for information security controls. INT'L ORG. FOR STANDARDIZATION, ISO 27002, SECURITY TECHNIQUES-CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS § 27002 (2013) [hereinafter ISO 27002]. It originated in a document published by the U.K. government, became a standard (BS7799) in 1995, was adopted as the International Standard ISO 17799 in 2000, and was renumbered in 2005 as ISO 27002. INT'L ORG. FOR STANDARDIZATION, ISO 27001, AN INTRODUCTION TO ISO 27001 (2005) [hereinafter ISO 27001]. The most recent 2013 version of ISO 27002 contains 114 security controls organized in fourteen sections. *See* ISO 27002. Though it contains voluntary guidance for organizations on information security controls, ISO 27002 also supports ISO 27001, which is an international standard for information security management systems, against which certification is granted. *See* ISO 27001. Currently over a thousand certificates of compliance with ISO 27001 are in place globally. *See id.*

[6] The National Institute of Standards and Technology (NIST) published its *Framework for Improving Critical Infrastructure Cybersecurity* on February 12, 2014. *See NIST Releases Cybersecurity Framework Version 1.0*, NAT'L INST. OF STANDARDS & TECH. (Feb. 12, 2014), http://www.NIST.gov/itl/csd/launch-cybersecurity-framework-021214.cfm, *archived at* http://perma.cc/7U3T-ZYU3. NIST developed the Cybersecurity Framework in response to Executive Order 13636: Improving Critical Infrastructure Cybersecurity, issued by President Obama in February 2013, which called for development of a voluntary, risk-based cybersecurity framework to help organizations manage cyber risks. *Id.* The NIST Cybersecurity Framework includes a Framework Core, which is an organization of specific cybersecurity activities and outcomes, with references to pertinent standards. *Id.* The Cybersecurity Framework also includes Framework Implementation Tiers and a Framework Profile, which together allow organizations to determine how best to assess and identify risks and apply controls consistent with the organization's objectives regarding cybersecurity. *Id.* The

reasonable information security program should include the following elements, with each element addressed in a manner consistent with the organization's applicable legal requirements, obligations to third-parties, and strategic approach to risk:

1. An organization should identify the types of information in its possession, custody, or control for which it will establish security safeguards ("Protected Information").
2. An organization should assess anticipated threats, vulnerabilities, and risks to the security of Protected Information.
3. An organization should establish and maintain appropriate policies and administrative, physical, and technical controls to address the identified threats, vulnerabilities, and risks to the security of Protected Information.
4. An organization should address the security of Protected Information in its third-party relationships.
5. An organization should respond to detected breaches of the security of Protected Information.

Framework Core organizes categories and subcategories of specific cybersecurity controls and activities in terms of five cybersecurity functions: identify, protect, detect, respond, and recover. *Id*.

The context of the Cybersecurity Framework is information security for "critical infrastructure," which has a broad footprint. *Id.* The Presidential Policy Directive on Critical Infrastructure Security and Resilience identifies sixteen critical infrastructure sectors in the United States, including Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. Press Release, The White House Office of the Press Secretary, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, *archived at* http://perma.cc/4NHZ-36E9.

6. An organization should periodically review and update its policies and controls for the security of Protected Information.

Although the absence of a reasonable information security program does not inexorably result in liability for the organization,[7] greater clarity

[7] For example, companies suffering data breaches have successfully defeated customer class action claims by relying on the Supreme Court's decision in *Clapper v. Amnesty International*, in which the court found plaintiffs lacked standing for failure to show actual harm or certainly impending injury. Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1148–51 (2013) (plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."). *See, e.g.*, *In re* Barnes & Noble Pin Pad Litig., 12-cv-8617, 2013 U.S. Dist. LEXIS 125730, at *11–12 (N.D. Ill. Sept. 3, 2013) (dismissing plaintiffs' claims for lack of standing, holding that an increased risk of fraud or identity theft did not satisfy actual injury requirement); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014) (holding allegations of possible future injury due to data breach, standing alone, are too speculative to confer standing, and expenses incurred to monitor and prevent identity theft held not to be actual injuries); Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 467–68 (D.N.J. 2013); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litg., No. 12-347 (JEB), 2014 U.S. Dist. LEXIS 64125, at *33 (D.D.C. May 9, 2014); Strautins v. Trustwave Holdings, Inc., No. 12 C 09115, 2014 U.S. Dist. LEXIS 32118, at *21–25 (N.D. Ill. Mar. 12, 2014). *But see In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014) (denying motion to dismiss, holding allegations of actual data breach and of theft and disclosure of plaintiffs' personal information are sufficient to establish certainly impending injury).

In the context of shareholder claims arising from data breaches, the business judgment rule shields corporate directors and officers from civil liability for decisions allegedly breaching the fiduciary duty of care, absent gross negligence. *See* Stone v. Ritter, 911 A.2d 362, 372 (Del. 2006). Shareholder claims based instead upon directors' and officers' alleged failure to exercise effective oversight are subject to the legal standards of *In re Caremark International Derivative Litigation* and its progeny. Such *Caremark* claims of oversight liability require the failure of directors and officers to act in good faith, resulting in a breach of the duty of loyalty. *Stone*, 911 A.2d at 369–70. For such liability to exist, the directors or officers must either fail "to implement any reporting or information system or controls; or [] having implemented such a system or controls, [they must] consciously fail[] to monitor or oversee . . . [their] operations," thereby preventing themselves from being informed of risks or problems that require their attention. *Id.* at 370. *See Palkon v. Holmes*, No.14-CV-01234, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014) (dismissing derivative action claims arising from Wyndham Worldwide Corporation's data security breaches).

regarding what constitutes a reasonable information security program would advance certainty for all concerned, and particularly for organizations operating, as they must, in a perilous information world.

II. THE RELEVANCE OF REASONABLENESS

[6] The concept of reasonableness pervades the law of information security. As discussed below, reasonableness is a common, unifying theme, from trade secret law protecting the organization's confidential business information to the various prescriptive legal schemes requiring safeguards for different types of protected information, as well as under the U.S.-EU Safe Harbor Privacy Principles and in FTC enforcement of information security.

A. Reasonableness and the Protection of Confidential Business Information

[7] Organizations rely on trade secret law for protection of confidential intellectual property. Trade secret status may exist for "all forms and types of financial, business, scientific, technical, economic, or engineering information," if such information has actual or potential economic value by being neither generally known to, nor readily accessible through proper means by, the public.[8] Trade secret status, however, only exists if "reasonable measures" are taken to maintain the information's secrecy.[9]

[8] 18 U.S.C. § 1839(3)(B) (2012); *see also* UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 538 (2005).

[9] 18 U.S.C. § 1839(3)(A) (2012) ("The owner therefore has taken reasonable measures to keep such information secret"); UNIF. TRADE SECRETS ACT § 1(4)(ii), 14 U.L.A. 538 (2005) ("is the subject of efforts that are reasonable under the circumstances to maintain its secrecy").

B. Reasonableness Under Laws Requiring Information Safeguards

1. Federal Information Security Laws

[8] The Security Rule under the Health Insurance Portability and Accountability Act ("HIPAA") is prescriptive in that HIPAA covered entities and business associates must comply with applicable standards and implementation specifications.[10] Nevertheless, the Security Rule's standards are grounded in reasonableness, both in the identification of risk and the application of security controls. Thus, fundamental requirements under the Security Rule include protection "against any reasonably anticipated threats or hazards to the security or integrity" of electronic protected health information, and "against any reasonably anticipated uses or disclosures of such information that are not permitted or required" under the HIPAA privacy rules.[11] For implementation of policies and controls, HIPAA requires covered entities and business associates to establish security measures "sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level . . . ."[12] Covered entities and business associates may therefore "use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified" in the Security Rule.[13] The security standards in the HIPAA Security Rule are accompanied by thirty-six implementation specifications, twenty-two of which are classified as "Addressable."[14] If an implementation specification is "Addressable," the covered entity or business associate

[10] *See* 45 C.F.R. § 164.302 (2013).

[11] 45 C.F.R. § 164.306(a)(2)–(3) (2013).

[12] 45 C.F.R. § 164.308(a)(1)(ii)(B) (2013).

[13] 45 C.F.R. § 164.306(b)(1) (2013).

[14] 45 C.F.R. pt. 164, subpt. C, app. A (2013).

must assess whether the implementation specification "is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting" ePHI.[15]

[9] The Gramm-Leach-Bliley Act requires regulators of financial institutions to establish standards for "administrative, technical, and physical safeguards" for "the security and confidentiality of customer records and information."[16] The resulting "Interagency Guidelines Establishing Information Security Standards," cooperatively promulgated by the respective federal banking agencies,[17] require such financial

[15] 45 C.F.R. § 164.306(d)(3)(i) (2013). If the implementation specification is "reasonable and appropriate," it must be implemented, and if such implementation would not be "reasonable and appropriate," the covered entity or business associate must document why it would not be so and must "[i]mplement an equivalent alternative measure if reasonable and appropriate." 45 C.F.R. § 164.306(d)(3)(ii) (2013).

[16] 15 U.S.C. §§ 6801(b), (b)(1) (2012).

[17] *See, e.g.*, 12 C.F.R. pt. 30, app. B (2014) (Office of Comptroller of the Currency ("OCC") standards applicable to "national banks, federal branches and federal agencies of foreign banks," and subsidiaries other than "brokers, dealers, persons providing insurance, investment companies, and investment advisers"); 12 C.F.R. pt. 170, app. B (2014) (OCC standards applicable to federal savings associations); 12 C.F.R. pt. 208, app. D-2 (2014) (Federal Reserve Board standards applicable to state member banks and their non-bank subsidiaries, "except for brokers, dealers, persons providing insurance, investment companies, and investment advisers"); 12 C.F.R. pt. 225, app. F (2014) (Federal Reserve Board standards applicable to bank holding companies and their non-bank subsidiaries or affiliates (except brokers, dealers, insurance providers, investment companies, and investment advisers) for which the Federal Reserve Board has supervisory authority); 12 C.F.R. pt. 364, app. B (2014) (Federal Deposit Insurance Corporation (FDIC) standards applicable to insured non-member banks, "insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers)").

The Board of the National Credit Union Administration has similar standards for safeguarding member information under Gramm-Leach-Bliley. *See* 12 C.F.R. pt. 748, app. A (2014). The Bureau of Consumer Financial Protection is explicitly not authorized to establish data security standards for financial institutions within its jurisdiction; *see also* 15 U.S.C. § 6801(b) (2012).

institutions to implement a comprehensive written information security program, with administrative, technical, and physical safeguards "appropriate to the size and complexity of the [entity] and the nature and scope of its activities."[18] When developing an information security program, the financial institution must first assess risk by identifying "reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems."[19]

[10] The Securities and Exchange Commission addresses safeguard standards under Gramm-Leach-Bliley for customer information retained by registered brokers, dealers, investment companies, and investment advisers in Regulation S-P, requiring the adoption of written policies and procedures to address administrative, technical, and physical safeguards for protecting customer records and information. Regulation S-P provides that such written policies and procedures must be "reasonably designed to":

> (1) Insure the security and confidentiality of customer records and information;
>
> (2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
>
> (3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[20]

[18] 12 C.F.R. pt. 30, app. B(II)(A) (2014).

[19] 12 C.F.R. pt. 30, app. B(III)(B)(1) (2014).

[20] 17 C.F.R. § 248.30(a)(1)–(3) (2014).

The FTC standards for safeguarding customer information, applicable to financial institutions not subject to the jurisdiction of the above agencies or authorities,[21] contain "standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[22] Under the FTC Safeguards Rule, the mandated comprehensive information security program must be developed by identifying "reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information . . . ."[23] The resulting information security program must also be "reasonably designed" to achieve the standard's objectives.[24]

[11] The Fair and Accurate Credit Transactions Act ("FACTA") requires the regulators of financial institutions to promulgate rules requiring the proper disposal of customer information derived from consumer reports for a business purpose.[25] Disposal Rules promulgated

[21] *See* 15 U.S.C. § 6805(a)(8) (2012). Safeguards standards under Gramm-Leach-Bliley for insurance providers are a matter of state insurance law, addressed by the applicable state insurance authorities. *See* 15 U.S.C. §§ 6801(b), 6805(a)(6) (2012).

[22] 16 C.F.R. § 314.1(a) (2014).

[23] 16 C.F.R. § 314.4(b) (2014).

[24] *See* 16 C.F.R. § 314.3(a) (2014).

[25] *See, e.g.*, 15 U.S.C. § 1681w(a)(1) (2012). Under FACTA, various federal agencies must also promulgate regulations requiring each financial institution and each creditor to "establish reasonable policies and procedures" to identify possible risks, or "red flags," of identity theft, potentially harmful to account holders, customers, or the institution. 15 U.S.C. § 1681m(e)(1)(B) (2012). The resulting Red Flags Rules of financial institution regulators require such institutions to establish an identity theft prevention program, which must include "reasonable policies and procedures" to identify relevant Red Flags for the covered accounts and incorporate them into the identity theft prevention program. *See, e.g.*, 16 C.F.R. § 681.1(a), 681.1(d)(1)–(2) (2014) (Federal Trade Commission's Red Flags Rule for financial institutions and creditors subject to administrative enforcement by the FTC). The same "reasonable policies and procedures" language is found in the Red Flags Rules of the OCC, 12 C.F.R. § 41.90(a), 41.90(d)(1)–(2) (2014) (national

under FACTA require persons who maintain or possess consumer information comprising or derived from a consumer report for a business purpose to properly dispose of such information "by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[26]

[12] The Children's Online Privacy Protection Act ("COPPA") requires the FTC to promulgate regulations requiring operators of websites or online services directed to children to establish and maintain "reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[27] Accordingly, the FTC's COPPA Rule succinctly provides that such operators "must establish and maintain

banks, federal savings associations, federal branches or agencies of foreign banks, or their operating subsidiaries); the Federal Reserve Board, 12 C.F.R. § 222.90(a), 222.90(d)(1)–(2) (2014) (Federal Reserve System member banks other than national banks and their operating subsidiaries, branches and agencies of foreign banks, and commercial lending companies owned or controlled by foreign banks); the FDIC, 12 C.F.R. § 334.90(a), 334.90(d)(1)–(2) (2014) (insured state non-member banks, insured state licensed branches of foreign banks, and their subsidiaries (except for brokers, dealers, insurance providers, investment companies, and investment advisers)); the National Credit Union Administration, 12 C.F.R. §§ 717.90(a), 717.90(d)(1)–(2) (2014) (federal credit unions); and the SEC, 17 C.F.R. §§ 248.201(a)(1)–(3), 248.201(d)(1)–(2) (2014) (registered brokers, dealers, investment companies, and investment advisers).

[26] 16 C.F.R. § 682.3(a) (2014). The Disposal Rules of other financial institution regulators contain the same "reasonable measures" language. *See* 17 C.F.R. § 248.30(b)(2) (2014) (SEC Disposal Rule for registered brokers, dealers, investment companies, and investment advisers). Other financial institution regulators have included their Disposal Rules in their Guidelines Establishing Information Security Standards including the OCC. *See, e.g.*, 12 C.F.R. § 41.83(b) (2014), 12 C.F.R pt. 30, app. B(III)(C)(4) (2014) (Comptroller of the Currency); 12 C.F.R. § 222.83(b) (2014), 12 C.F.R. pt. 208, app. D-2(III)(C)(4) (2014) (Federal Reserve System); 12 C.F.R. § 334.83(a) (2014), 12 C.F.R. pt. 364, app. B(III)(C)(4) (2014) (Federal Deposit Insurance Corporation); 12 C.F.R. § 717.83(a) (2014), 12 C.F.R. pt. 748, app. A(III)(C)(4) (2014) (National Credit Union Administration).

[27] 15 U.S.C. § 6502(b)(1)(D) (2012).

reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[28]

2. State Information Security Laws

[13] Various states affirmatively require persons and businesses possessing protected personally identifiable information ("PII") of state residents to implement and maintain "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[29] Persons who own or license personal information about Massachusetts' residents must maintain a written comprehensive information security program with administrative, technical, and physical safeguards that are

> Appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and

[28] 16 C.F.R. § 312.8 (2014).

[29] *See, e.g.*, ARK. CODE ANN. § 4-110-104(b) (Supp. 2011); *see also* CAL. CIV. CODE § 1798.81.5(b) (Deering Supp. 2014) ("implement and maintain reasonable security procedures and practices"); MD. CODE ANN., COM. LAW § 14-3503(a) (LexisNexis Supp. 2013) ("implement and maintain reasonable security procedures and practices"); NEV. REV. STAT. § 603A.210(1) (LexisNexis Supp. 2010) ("implement and maintain reasonable security measures"); OR. REV. STAT. § 646A.622(1) (West 2011) ("develop, implement and maintain reasonable safeguards"); R.I. GEN. LAWS § 11-49.2-2(2) (Supp. 2013) ("implement and maintain reasonable security procedures and practices"); UTAH CODE ANN. § 13-44-201(1) (LexisNexis 2013) ("implement and maintain reasonable procedures"). Effective July 1, 2014, the Florida Information Protection Act of 2014 requires commercial entities that acquire, maintain, store, or use PII—and also entities contracted to maintain, store, or process PII on their behalf—to "take reasonable measures to protect and secure" electronic PII. FLA. STAT. ANN. § 501.171(2) (2014).

> confidentiality of both consumer and employee information.[30]

[14] A majority of states have laws requiring entities with PII of state residents to take reasonable measures to protect such information when it is disposed of or discarded. Alaska, Colorado, Hawaii, North Carolina, and Oregon require such entities to have a disposal policy for PII.[31] Other states specify compliant means of reasonable PII disposal, such as shredding of hardcopy documents, effective erasure of electronic media, or other similar actions that render PII unreadable or indecipherable.[32]

---

[30] 201 MASS. CODE REGS. 17.03(1)(a)–(d) (2013). Though some of the Massachusetts standards' requirements are unambiguously prescriptive, the standards incorporate reasonableness, such as in program development through identifying and assessing "reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, . . . [taking] reasonable steps to select and retain third-party service providers, . . . [establishing] [r]easonable restrictions upon physical access . . . "; performing regular monitoring to ensure that the program is "operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information . . . "; and "[r]eviewing the scope of security measures . . . whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information." 201 MASS. CODE REGS. 17.03(2)(b), (2)(f)(1), (2)(g)–(i) (2013). The Massachusetts requirements for computer system security similarly employ reasonableness in requirements regarding assignment and selection of passwords, system monitoring, firewall protection, and system security agent software. *See* 201 MASS. CODE REGS. 17.04(1)(b), (4), (6)–(7) (2014).

[31] *See* ALASKA STAT. § 45.48.530 (2012); COLO. REV. STAT. § 6-1-713(1) (2013); HAW. REV. STAT. ANN. § 487R-2(a), (b)(1)–(3) (LexisNexis Supp. 2012); N.C. GEN. STAT. § 75-64(a)-(b)(1)–(3) (2013); OR. REV. STAT. ANN. § 646A.622(2)(a)–(c) (West 2011).

[32] *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7601(A)–(C) (2013); ARK. CODE ANN. § 4-110-104(a) (Supp. 2011); CAL. CIV. CODE § 1798.81 (Deering Supp. 2014); CONN. GEN. STAT. § 42-471(a) (2013); FLA. STAT. ANN. § 501.171(8) (2014); GA. CODE ANN. § 10-15-2 (2009); IND. CODE ANN. § 24-4-14-8 (2013); KAN. STAT. ANN. § 50-7a03 (Supp. 2013); KY. REV. STAT. ANN. § 365.725 (LexisNexis 2008); MD. CODE ANN., COM. LAW § 14-3502(b) (LexisNexis Supp. 2013); MASS. GEN. LAWS ch. 93H, § 2(a)–(b) (2012); MONT. CODE ANN. § 30-14-1703 (2013); NEV. REV. STAT. ANN. § 603A.200(1)–(2) (LexisNexis Supp. 2010); N.J. STAT. ANN. § 56:8-162 (West 2012); N.Y. GEN. BUS. LAW § 399-h(2) (Consol. 2014); S.C. CODE ANN. § 37-20-190(A)–(B) (Supp. 2013); TEX.

[15] California, Maryland, Nevada, and Rhode Island require businesses that disclose state residents' PII to non-affiliated third-parties to have contracts obligating such third-parties to establish reasonable PII security procedures and practices.[33] Massachusetts and Oregon mandate information security programs that, among other matters, require appropriate PII protection to be addressed in service provider contracts.[34] And Alaska, Hawaii, and North Carolina have similar requirements for reasonable security measures in arrangements with service providers for PII disposal.[35]

3. Reasonableness under the U.S.-EU Safe Harbor Framework

[16] The U.S.-EU Safe Harbor Framework, developed by the U.S. Department of Commerce, is the vehicle through which United States' organizations can participate in the transfer of personal data protected by the European Commission's Directive on Data Protection. [36]

BUS. & COM. CODE ANN. § 521.052(b) (West Supp. 2013); UTAH CODE ANN. § 13-44-201(1)–(2) (Supp. 2013); VT. STAT. ANN. tit. 9, § 2445(b) (2006); WASH. REV. CODE § 19.215.020(1) (2014); WIS. STAT. § 134.97(2) (2012) (financial institutions, medical businesses, or tax preparation businesses).

[33] *See* CAL. CIV. CODE § 1798.81.5(c) (Deering Supp. 2014); MD. CODE ANN., COM. LAW § 14-3503(b)(1)(i)–(ii) (LexisNexis Supp. 2013); NEV. REV. STAT. ANN. § 603A.210(2) (LexisNexis Supp. 2010); R.I. GEN. LAWS § 11-49.2-2(3) (Supp. 2013).

[34] *See* 201 MASS. CODE REGS. 17.03(2)(f)(2) (2012); OR. REV. STAT. ANN. § 646A.622(2)(d)(A)(v) (West 2011).

[35] *See, e.g.*, ALASKA STAT. § 45.48.510(3) (2012); HAW. REV. STAT. ANN. § 487R-2(c) (LexisNexis Supp. 2012); N.C. GEN. STAT. § 75-64(c) (2013). *But see* 815 ILL. COMP. STAT. § 530/40(c) (2012) (no reasonableness standard for provisions of disposal provider contracts); S.C. CODE ANN. § 37-20-190(B) (Supp. 2013) (no reasonableness standard for provisions of disposal provider contracts).

Organizations in the United States may voluntarily apply for Safe Harbor status by publicly declaring that they are and will be in compliance with the U.S.-EU Safe Harbor Framework's requirements, and stating in their published privacy policies that they will adhere to the seven Safe Harbor Privacy Principles.[37] Safe Harbor enforcement is primarily administered by the private sector, but certain regulators, including the FTC can enforce compliance through prohibitions against unfair and deceptive trade practices.[38] Under the Safe Harbor's Security Principle, "[o]rganizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction."[39]

4. Reasonableness under Section 5 of the FTC Act

[17] The FTC has enforcement authority under several of the above-referenced laws requiring security programs, including Gramm-Leach-Bliley,[40] FACTA,[41] and COPPA.[42] Because FTC regulations issuing from these statutes are couched in terms of reasonableness, FTC enforcement consent orders, unsurprisingly, incorporate a reasonableness standard as well. FTC orders in enforcement matters under the Gramm-Leach-Bliley Security Rule commonly compel the respondent company to establish "a comprehensive information security program that is reasonably designed

[36] *See U.S.-EU Safe Harbor Overview,* EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last visited Nov. 3, 2014), *archived at* http://perma.cc/P5DL-Y48Z.

[37] *See id.*

[38] *See id.*

[39] *Id.*

[40] *See* 15 U.S.C. § 6805(a)(7) (2012).

[41] *See* 15 U.S.C. § 1681w(a)(1) (2012).

[42] *See* 15 U.S.C. § 6502(b)(1) (2012).

to protect the security, confidentiality, and integrity of personal information" of consumers.[43] In one FACTA disposal rule enforcement

[43] *See, e.g.*, Consent Order at 2–3, *In re* ACRAnet, Inc., No. C-4331 (F.T.C. Aug. 17, 2011) [hereinafter ACRAnet Order], http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110809acranetdo.pdf, *archived at* http://perma.cc/Y8JS-F3XY; Consent Order at 3, *In re* Fajilan & Assocs., No. C-4332 (F.T.C. Aug. 17, 2011) [hereinafter Fajilan Order], http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819statewidedo.pdf, *archived at* http://perma.cc/ACL8-52FH; Consent Order at 3, *In re* Franklin's Budget Car Sales, Inc., No. C-4371 (F.T.C. Oct. 3, 2012) [hereinafter Franklin's Budget Car Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026franklinautomalldo.pdf, *archived at* http://perma.cc/GN9L-JL86; Consent Order at 3, *In re* Goal Financial, LLC, No. C-4216 (F.T.C. Apr. 9, 2008) [hereinafter Goal Financial Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/04/080415decision_0.pdf, *archived at* http://perma.cc/Z5LF-HEUW; Consent Order at 2, *In re* James B. Nutter & Co., No. C-4258 (F.T.C. June 12, 2009) [hereinafter James B. Nutter & Co. Order], http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090616nutterdo.pdf, *archived at* http://perma.cc/887F-PURA; Consent Order at 3, *In re* Nations Title Agency, Inc., No. C-4161 (F.T.C. June 19, 2006) [hereinafter Nations Title Agency Order], http://www.ftc.gov/sites/default/files/documents/cases/2006/06/0523117nationstitledecisionandorder.pdf, *archived at* http://perma.cc/D9VY-ZESP; Consent Order at 3, *In re* Premier Capital Lending, Inc., No. C-4241 (F.T.C. Dec. 10, 2008) [hereinafter Premier Capital Lending Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081216pcldo.pdf, *archived at* http://perma.cc/2XQ9-PL7E; Consent Order at 3, *In re* SettlementOne Credit Corp. & Sackett Nat'l Holdings, Inc., No. C-4330 (F.T.C. Aug. 17, 2011) [hereinafter SettlementOne Credit and Sackett National Holdings Order], http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonedo.pdf, *archived at* http://perma.cc/7XCG-JEU4.

Early FTC enforcement consent orders under the Gramm-Leach-Bliley Safeguards Rule instead simply prohibited future violation of the Safeguards Rule, coupled with periodic assessments by a qualified, independent third-party professional to certify that the security program is operating with sufficient effectiveness "to provide reasonable assurance that the security, confidentiality, and integrity of personal information" is being protected. *See, e.g.*, Consent Order at 5–6, United States v. Am. United Mortg. Co., No. 07C-7064 (N.D. Ill. Dec. 17, 2007) [hereinafter American United Order], http://www.ftc.gov/sites/default/files/documents/cases/2007/12/071217americanunitedmrtgstipfinal.pdf, *archived at* http://perma.cc/SY2V-837H; Consent Order at 2–3, *In re* Nationwide Mortg. Grp., Inc., No. 9319 (F.T.C. Apr. 12, 2005) [hereinafter Nationwide Order],

proceeding, the FTC's consent order permanently enjoined the defendant from violating the Disposal Rule, including any failure "to properly dispose of such information by taking reasonable measures to protect against unauthorized access to use of the information in connection with its disposal."[44] And in COPPA enforcement, the FTC has prohibited a respondent from "failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children," and has ordered the establishment of "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of consumer personal information . . . ."[45]

[18] For over a decade, the majority of the FTC's information security enforcement proceedings have been brought under Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[46] Under the authority of Section 5,

---

http://www.ftc.gov/sites/default/files/documents/cases/2005/04/050415dod9319.pdf, *archived at* http://perma.cc/J6QA-V3TV; Consent Order at 2–3, *In re* Sunbelt Lending Servs., Inc., No. C-4129 (F.T.C. Jan. 3, 2005) [hereinafter Sunbelt Lending Order], http://www.ftc.gov/sites/default/files/documents/cases/2005/01/050107do0423153.pdf, *archived at* http://perma.cc/J6QA-V3TV.

[44] *See, e.g.*, Consent Order at 6, FTC v. Navone, No. 2:08-CV-01842 (D. Nev. Dec. 29, 2009) [hereinafter Navone Order], http://www.ftc.gov/sites/default/files/documents/cases/2010/01/100120navonestip.pdf, *archived at* http://perma.cc/S396-YLVK.

[45] *See* Consent Order at 5, 8, *In re* RockYou, Inc., No. 12-CV-1487 (F.T.C. Mar. 27, 2012) [hereinafter RockYou Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf. *archived at* http://perma.cc/9AUR-RBB9; s*ee also* Consent Order at 12–13, United States v. Path, Inc., No. 13-CV-00448-RS (N.D. Cal. Feb. 8, 2013) [hereinafter Path Order], http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf (ordering defendant to establish and maintain "a comprehensive privacy program that is reasonably designed to . . . protect the privacy and confidentiality of covered information"), *archived at* http://perma.cc/Y8V4-LTPH.

[46] 15 U.S.C. § 45(a)(1) (2012).

the FTC enforces information security through one or a combination of two prohibitions. First, if a company makes representations—such as statements within its privacy policy—that it will maintain particular safeguards or provide a certain level of security for customer information, yet fails to do so, the FTC may proceed under the deceptiveness prong of Section 5.[47] Conversely, without reference to any alleged misrepresentation regarding information security, the FTC may instead pursue a company under the unfairness prong of Section 5.[48] In an unfairness claim, however, the FTC must also allege and establish that "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[49] In at least fifteen concluded enforcement matters in the last twelve years, the FTC has pursued companies solely under a Section 5 deception theory, with no companion claims under Gramm-Leach-Bliley, FACTA, or COPPA, and therefore with no underlying, specific regulatory standards for prescribed safeguards.[50] In each of these matters the

[47] *See, e.g.*, Complaint at 5, *In re* Twitter, Inc., No. C-4316 (F.T.C. Mar. 2, 2011) [hereinafter Twitter Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf, *archived at* http://perma.cc/B7MB-EXCR.

[48] *See, e.g.*, Complaint at 3, *In re* Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010) [hereinafter Dave & Buster's Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2010/06/100608davebusterscmpt.pdf.

[49] 15 U.S.C. § 45(n) (2012)*; see, e.g.*, Dave & Buster's Complaint at 3.

[50] *See, e.g.*, Complaint at 11–14, FTC v. LifeLock, Inc., No. 072-3069 (D. Ariz. Mar. 8, 2010) [hereinafter LifeLock Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf, *archived at* http://perma.cc/A98N-JT5D; Complaint at 13–14, United States v. ValueClick, Inc., No. CV08-01711 MMM (RZx) (C.D. Cal. Mar. 13, 2008) [hereinafter ValueClick Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317complaint.pdf, *archived at* http://perma.cc/4T9R-5Y3H; Complaint at 4, *In re* Cbr Sys., Inc., No. C-4400 (F.T.C. Apr. 29, 2013) [hereinafter Cbr Systems Complaint],

resulting consent order required the company to establish a comprehensive information security program that is "reasonably designed to protect the security, confidentiality, and integrity" of consumer information.[51] During

http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrcmpt.pdf, *archived at* http://perma.cc/T2LS-TDTP; Complaint at 5–6, *In re* Credit Karma, Inc., No. C-4480 (F.T.C. Aug. 13, 2014) [hereinafter Credit Karma Complaint], http://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf, *archived at* http://perma.cc/NL4H-AXFH; Complaint at 3, *In re* Eli Lily & Co., No. C-4047 (F.T.C. May 8, 2002) [hereinafter Eli Lily Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2002/05/elililllycmp.htm, *archived at* http://perma.cc/A9UT-FMYV; Complaint at 5, *In re* Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014) [hereinafter Fandango Complaint], http://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf, *archived at* http://perma.cc/93CF-9LYT; Complaint at 3, *In re* Genica Corp., No. C-4252 (F.T.C. Mar. 16, 2009) [hereinafter Genica Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090320genicacmpt.pdf, *archived at* http://perma.cc/KR2Q-QJVA; Complaint at 3, *In re* Guess?, Inc., No. C-4091 (F.T.C. July 30, 2003) [hereinafter Guess Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2003/08/guesscomp.pdf, *archived at* http://perma.cc/6PRC-ZJ5P; Complaint at 3, *In re* Guidance Software, Inc., No. C-4187 (F.T.C. Mar. 30, 2007) [hereinafter Guidance Software Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2007/04/0623057complaint.pdf, *archived at* http://perma.cc/WC6Y-ZSL7; Complaint at 3, *In re* Life is Good, Inc., No. C-4218 (F.T.C. Apr. 16, 2008) [hereinafter Life is Good Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2008/04/080418complaint.pdf, *archived at* http://perma.cc/G9W3-4Y32; Complaint at 5, *In re* Microsoft Corp., No. C-4069 (F.T.C. Dec. 20, 2002) [hereinafter Microsoft Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2002/08/microsoftcmp.pdf, *archived at* http://perma.cc/8GSM-ZJSX; Complaint at 4, *In re* MTS, Inc. & Tower Direct, LLC, No. C-4110 (F.T.C. May 28, 2004) [hereinafter MTS and Tower Direct Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2004/06/040602comp0323209.pdf, *archived at* http://perma.cc/VV56-DQPN; Complaint at 5-6, 8, *In re* Myspace LLC, No. C-4369 (F.T.C. Aug. 30, 2012) [hereinafter Myspace Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacecmpt.pdf (also alleging misrepresentations regarding U.S. Safe Harbor adherence), *archived at* http://perma.cc/M2QB-FRWZ; Complaint at 4, *In re* Petco Animal Supplies, Inc., No. C-4133 (F.T.C. Mar. 4, 2004) [hereinafter Petco Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2005/03/050308comp0323221.pdf, *archived at* http://perma.cc/YSW7-4DUY; Twitter Complaint at 5.

[51] *See, e.g.*, Consent Order at 5, FTC v. LifeLock, Inc., No. 072-3069 (D. Ariz. Mar. 9, 2010) [hereinafter LifeLock Order], http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockstip.pdf, *archived at* http://perma.cc/M55H-ZMHX; Consent Order at 9–10, United States v. ValueClick, Inc., No. CV08-01711 MMM (RZx) (C.D. Cal. Mar. 17, 2008) [hereinafter ValueClick Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317judgment.pdf, *archived at* http://perma.cc/J5EG-J8H6; Consent Order at 3, *In re* Cbr Systems, Inc., No. C-4400 (F.T.C. Apr. 29, 2013) [hereinafter Cbr Systems Order], http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrdo.pdf, *archived at* http://perma.cc/9ZZZ-SD5T; Consent Order at 3, *In re* Credit Karma, Inc., No. C-4480 (F.T.C. Aug. 13, 2014) [hereinafter Credit Karma Order], http://www.ftc.gov/system/files/documents/cases/1408creditkarmado.pdf, *archived at* http://perma.cc/T66M-F539; Consent Order at II., *In re* Eli Lily & Co., No. C-4047 (F.T.C. May 8, 2002) [hereinafter Eli Lily Order], http://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillydo.htm, *archived at* http://perma.cc/9PUG-6F5T; Consent Order at 3, *In re* Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014) [hereinafter Fandango Order], http://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf, *archived at* http://perma.cc/3RTB-SEDK; Consent Order at 3, *In re* Genica Corp., No. C-4252 (F.T.C. Mar. 16, 2009) [hereinafter Genica Order], http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090320genicado.pdf, *archived at* http://perma.cc/Q7A3-QMC2; Consent Order at 3, *In re* Guess?, Inc., No. C-4091 (F.T.C. July 30, 2003) [hereinafter Guess Order], http://www.ftc.gov/sites/default/files/documents/cases/2003/08/guessdo.pdf, *archived at* http://perma.cc/XWG3-EKXP; Consent Order at 2–3, *In re* Guidance Software, Inc., No. C-4187 (F.T.C. Mar. 30, 2007) [hereinafter Guidance Software Order], http://www.ftc.gov/sites/default/files/documents/cases/2007/04/0623057do.pdf, *archived at* http://perma.cc/6FSC-ZTK2; Consent Order at 3, *In re* Life is Good, Inc., No. C-4218 (F.T.C. Apr. 16, 2008) [hereinafter Life is Good Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/04/080418do.pdf, *archived at* http://perma.cc/R7QA-WAFF; Consent Order at 2–3, *In re* Microsoft Corp., No. C-4069 (F.T.C. Dec. 20, 2002) [hereinafter Microsoft Order], http://www.ftc.gov/sites/default/files/documents/cases/2002/12/microsoftdecision.pdf, *archived at* http://perma.cc/N88X-WDCT; Consent Order at 3, *In re* MTS, Inc., & Tower Direct, LLC, No. C-4110 (F.T.C. May 28, 2004) [hereinafter MTS and Tower Direct Order], http://www.ftc.gov/sites/default/files/documents/cases/2004/06/040602do0323209.pdf, *archived at* http://perma.cc/AC24-5PH2; Consent Order at 3, *In re* Myspace LLC, No. C-4369 (F.T.C. Aug. 30, 2012) [hereinafter Myspace Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacedo.pdf, , *archived at* http://perma.cc/KXU7-RDF5; Consent Order at II., *In re* Petco Animal

the same time period, the FTC alleged Section 5 information security violations under a combination of deception and unfairness theories in twelve concluded enforcement matters, and the resulting consent orders similarly, and uniformly, compelled the company to establish a comprehensive information security program "reasonably designed to protect the security, confidentiality, and integrity" of such information.[52]

Supplies, Inc., No. C-4133 (F.T.C. Mar. 4, 2005) [hereinafter Petco Order], http://www.ftc.gov/sites/default/files/documents/cases/2005/03/050308do0323221.pdf, *archived at* http://perma.cc/8AZX-64JE; Consent Order at 3, *In re* Twitter, Inc., No. C-4316 (F.T.C. Mar. 2, 2014) [hereinafter Twitter Order], http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf, *archived at* http://perma.cc/22VL-ZPSJ.

[52] *See, e.g.*, Consent Order at 3, *In re* Ceridian Corp., No. C-4325 (F.T.C. June 8, 2011) [hereinafter Ceridian Corp. Order], http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110615ceridiando.pdf, *archived at* http://perma.cc/6P5Q-J8B5; Consent Order at 7, *In re* Compete, Inc., No. C-4384 (F.T.C. Feb. 20, 2013) [hereinafter Compete Order], http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competedo.pdf, *archived at* http://perma.cc/YV6U-3LKU; Consent Order at 3, *In re* CVS Caremark Corp., No. C-4259 (F.T.C. June 18, 2009) [hereinafter CVS Order], http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvsdo.pdf, *archived at* http://perma.cc/BZ7X-MSS8; Consent Order at 5, *In re* Facebook, LLC, No. C-4365 (F.T.C. July 27, 2012) [hereinafter Facebook Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf, *archived at* http://perma.cc/834G-6G33; Consent Order at 7, *In re* GeneLink, Inc., No. C-4456 (F.T.C. May 8, 2014) [hereinafter GeneLink Order], http://www.ftc.gov/system/files/documents/cases/140512genelinkdo_0.pdf, *archived at* http://perma.cc/49DZ-W9PU; Consent Order at 3, *In re* GMR Transcription Services, Inc., No. C-4482 (F.T.C. Aug. 14, 2014) [hereinafter GMR Transcription Services Order], http://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf, *archived at* http://perma.cc/CW6G-Y7XM; Consent Order at 3, *In re* HTC America, Inc., No. C-4406 (F.T.C. June 25, 2013) [hereinafter HTC America Order], http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf, *archived at* http://perma.cc/Q42M-9FX2; Consent Order at 3, *In re* Lookout Servs., Inc., No. C-4326 (F.T.C. June15, 2011) [hereinafter Lookout Services Order], http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110615lookoutdo.pdf, *archived at* http://perma.cc/NM4Z-33N6; Consent Order at 3, *In re* Rite Aid, Corp., No. C-4308 (F.T.C. Nov. 12, 2010) [hereinafter Rite Aid Order], http://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaiddo.pdf,

Notably, in at least eight concluded enforcement matters the FTC has pursued companies for allegedly inadequate information security solely under the unfairness prong of Section 5. These matters are of particular interest because the FTC's enforcement claims were neither based on specific regulatory standards under Gramm-Leach-Bliley, FACTA, or COPPA, nor allegedly deceptive representation regarding security safeguards. In each matter the FTC claimed that a failure to provide "reasonable and appropriate" security for protected consumer information constituted an unfair act or practice in violation of Section 5.[53] The

archived at http://perma.cc/8HD5-RH9C; Consent Order at 4, *In re* TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014) [hereinafter TRENDnet Order], http://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf, *archived at* http://perma.cc/N6D3-SVRM; Consent Order at 6, *In re* Upromise, Inc., No. C-4351 (F.T.C. Mar. 27, 2012) [hereinafter Upromise Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisedo.pdf, *archived at* http://perma.cc/GRK2-H6QD.

[53] *See, e.g.*, Complaint at 2, *In re* Accretive Health, Inc., No. C-4432 (F.T.C. Feb. 5, 2014) [hereinafter Accretive Health Complaint], http://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf ("Accretive failed to provide reasonable and appropriate security for consumers' personal information it collected and maintained by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access."), *archived at* http://perma.cc/E2G3-VP4G; Complaint at 2, *In re* BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005) [hereinafter BJ's Wholesale Club Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf ("Respondent did not employ reasonable and appropriate measures to secure personal information collected at its stores."), *archived at* http://perma.cc/WRK4-ZYBJ; Complaint at 2, *In re* CardSystems Solutions, Inc., No. C-4168 (F.T.C. Sept. 5, 2006) [hereinafter CardSystems Solutions Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2006/02/0523148complaint.pdf ("Respondent . . . failed to provide reasonable and appropriate security for personal information stored on its computer network."), *archived at* http://perma.cc/ZVD7-355B; Dave & Buster's Complaint at 2 ("In collecting and processing sensitive personal information, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its networks."); Complaint at 2, *In re* DSW Inc., No. C-4157 (F.T.C., Mar. 7, 2006) [hereinafter DSW Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2005/12/051201comp0523096.pdf

consent orders in each of these concluded enforcement matters, true to form, required the company to establish and maintain a comprehensive information security program "reasonably designed to protect the security, confidentiality, and integrity" of collected consumer personal information.[54]

("[R]espondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information collected at its stores."), *archived at* http://perma.cc/X7EK-64T7; Complaint at 2, *In re* EPN, Inc., No. C-4370 (F.T.C. Oct. 3, 2012) [hereinafter EPN Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf ("EPN has engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computers and networks."), *archived at* http://perma.cc/V3FJ-JVR8; Complaint at 3, *In re* Reed Elsevier, Inc., No. C-4226 (F.T.C. July 29, 2008) [hereinafter Reed Elsevier Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080327complaint.pdf ("[R]espondents engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to prevent unauthorized access to the sensitive consumer information stored in databases accessible using Accurint verification products . . . ."), *archived at* http://perma.cc/NJH4-A55Y; Complaint at 2, *In re* TJX Cos., No. C-4227 (F.T.C. July 29, 2008) [hereinafter TJX Cos. Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080327complaint_0.pdf ("[R]espondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on it networks."), *archived at* http://perma.cc/9G6Y-KFTE.

In its pending enforcement matter against LabMD, the FTC complaint similarly alleges that LabMD "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." *See* Complaint at 3, *In re* LabMD, Inc., No. 9357 (F.T.C. Aug. 28, 2013) [hereinafter LabMD Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf, *archived at* http://perma.cc/BNL7-2NTU.

[54] *See, e.g.*, Consent Order at 2–3, *In re* Accretive Health, Inc., No. C-4432 (F.T.C. Feb. 5, 2014) [hereinafter Accretive Health Order], http://www.ftc.gov/system/files/documents/cases/140224accretivehealthdo.pdf, *archived at* http://perma.cc/6ZRT-G79C; Consent Order at 2–3, *In re* BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005) [hereinafter BJ's Wholesale Club Order], http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305do0423160.pdf, *archived at* http://perma.cc/A427-CC4A; Consent Order at 3, *In re* Cardsystems Solutions, Inc., No. C-4168 (F.T.C. Sept. 5, 2006) [hereinafter Cardsystems Solutions

[19] The FTC's information security enforcement under Section 5's unfairness theory has engendered controversy.[55] In *FTC v. Wyndham*, the United States District Court for the District of New Jersey recently granted leave for an interlocutory appeal to the Third Circuit Court of Appeals on two certified questions:

> (1) Whether the Federal Trade Commission can bring an unfairness claim involving data security under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a); and
>
> (2) Whether the Federal Trade Commission must formally promulgate regulations before bringing its unfairness claim under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a).[56]

Order], http://www.ftc.gov/sites/default/files/documents/cases/2006/09/0523148cardsystemsdo.pdf, *archived at* http://perma.cc/9VNW-SYLS; Consent Order at 2–3, *In re* Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010) [hereinafter Dave & Buster's Order], http://www.ftc.gov/sites/default/files/documents/cases/2010/06/100608davebustersdo.pdf, *archived at* http://perma.cc/4D6L-6V7Z; Consent Order at 2–3, *In re* DSW Inc., No. C-4157 (F.T.C. Mar. 7, 2006) [hereinafter DSW Order], http://www.ftc.gov/sites/default/files/documents/cases/2006/03/0523096c4157dswdecisionandorder.pdf, *archived at* http://perma.cc/QF8B-LP2N; Consent Order at 2–3, *In re* EPN, Inc., No. C-4370 (F.T.C. Oct. 3, 2012) [hereinafter EPN Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epndo.pdf, *archived at* http://perma.cc/SYS9-9Z77; Consent Order at 3–4, *In re* Reed Elsevier, Inc., No. C-4226 (F.T.C. July 29, 2008) [hereinafter Reed Elsevier Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reeddo.pdf, *archived at* http://perma.cc/8VSV-PZ39; Consent Order at 2–3, *In re* TJX Cos., No. C-4227 (F.T.C. July 29, 2008) [hereinafter TJX Cos. Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxdo.pdf, *archived at* http://perma.cc/G2TN-9B7U.

[55] *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (discussing how the FTC has used Section 5 to fill a void in sector-specific privacy and data security law).

[20] Regardless of the ultimate result of opposition to the FTC's Section 5 enforcement authority, reasonableness remains ubiquitous in other expressions of information security law; and so the question of what constitutes a reasonable information security program still merits an answer.

III. ELEMENTS OF A REASONABLE INFORMATION SECURITY PROGRAM

[21] Information security is simply not a "one size fits all" endeavor. Different organizations in different industries face different threats, vulnerabilities, and risks for information security,[57] and such organizations inherently have different sizes, operating environments, and security capabilities. Also, security threats are not static, but instead evolve over time and may indeed emerge or shift rapidly.[58]

[56] FTC v. Wyndham Worldwide Corp., No. 13-1887 (ES), 2014 U.S. Dist. LEXIS 84914, at *15 (D.N.J. June 23, 2014) (order certifying questions for interlocutory review).

[57] Verizon's *2014 Data Breach Investigations Report* analyzed the frequency of security incident patterns over the last three years, by industry. This analysis revealed significant industry differences in the nature of security incidents. For example, the top three incident patterns for the Retail industry were Denial of Service, Point-of-Sale Intrusion, and Web App Attack. The most prevalent three incident patterns for the Healthcare industry were Theft/Loss, Insider Misuse, and Miscellaneous Error. For the Utilities industry, the top three patterns were Web App Attack, Crime-Ware, and Denial of Service. The three most frequent incident patterns for the Professional industry were Denial of Service, Cyber-espionage, and Web App Attack. And in the Accommodation industry, the frequency of Point-of-Sale Intrusion dwarfed all other incident patterns. *See 2014 Data Breach Investigations Report*, VERIZON 15 (2014), *available at* http://www.verizonenterprise.com/DBIR/2014/, *archived at* http://perma.cc/S9DD-Z7U8.

[58] The 2014 Verizon Report also compares the most prevalent varieties of security threat actions per year. In 2009, the most frequently occurring threat actions were Spyware/Key Logger (malware), Backdoor (malware), Use of Stolen Credentials (hacking), and Capture Stored Data (malware). In contrast, for 2013 the most prevalent threat actions were Use of Stolen Credentials (hacking), Export Data (malware), Phishing (social engineering), and RAM Scraper (malware). *See id.* at 10.

[22] Recognizing this diversity of circumstances, most information security laws explicitly allow for flexibility in establishing security safeguards for information. Under such laws, factors to be considered in establishing reasonable security safeguards include:

- The organization's size and complexity, and the nature and scope of its activities;[59]

- The organization's information security capabilities;[60]

- The organization's available resources and the costs of security measures;[61]

[59] *See* 12 C.F.R. pt. 30, app. B(II) (2014) ("appropriate to the size and complexity of the institution and the nature and scope of its activities.") (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); 12 C.F.R. pt. 748, app. A(II)(A) (2014) ("appropriate to the size and complexity of the credit union and the nature and scope of its activities.") (NCUA Guidelines for Safeguarding Member Information under Gramm-Leach-Bliley); 16 C.F.R. § 314.3(a) (2014) ("appropriate to your size and complexity [and] the nature and scope of your activities . . . .") (FTC Safeguards Rule under Gramm-Leach-Bliley); 45 C.F.R. § 164.306(b)(2)(i) (2013) ("[t]he size, complexity, and capabilities of the covered entity or business associate.") (HIPAA Security Rule); *see also* 201 MASS. CODE REGS. 17.03(1) (2013) (appropriate to "the size, scope and type of business of the person obligated to safeguard the personal information . . . .") (Massachusetts Standards for Protection of PII); OR. REV. STAT. § 646A.622(4) (West 2011) ("appropriate to the size and complexity of the small business [and] the nature and scope of its activities . . . .") (Oregon PII Safeguards Statute).

[60] *See, e.g.*, 45 C.F.R. § 164.306(b)(2)(ii) (2013) ("[t]he covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.") (HIPAA Security Rule).

[61] *See, e.g.*, 45 C.F.R. § 164.306(b)(2)(iii) (2013) ("[t]he costs of security measures.") (HIPAA Security Rule); 201 MASS. CODE REGS. 17.03(1)(b) (2014) ("appropriate to . . . the amount of resources available to such person . . . .") (Massachusetts Standards for Protection of PII).

On the other hand, the FTC has taken the position in its data security enforcement proceedings that some security safeguards are to be expected due to their ready availability, allegedly low cost, and common use. Thus, the FTC has found fault with

companies' failure to implement what it characterizes as readily available, free or low-cost defenses to commonly known or reasonably foreseeable attacks, such as SQL (Structured Query Language) injection attacks and XSS (Cross-Site Scripting) attacks. *See, e.g.*, Complaint at 2, *In re* Ceridian Corp., No. C-4325 (F.T.C. June 8, 2011) [hereinafter Ceridian Corp. Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110615ceridiancmpt.pdf, *archived at* http://perma.cc/9YYT-5JAS; Genica Complaint at 2; Life is Good Complaint at 2; LifeLock Complaint at 10; Complaint at 2, *In re* Nations Title Agency, Inc., No. C-4161 (F.T.C. June 19, 2006) [hereinafter Nations Title Agency Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2006/06/0523117nationstitle_complaint.pdf, *archived at* http://perma.cc/9N63-5HXG; Reed Elsevier Complaint at 4. The FTC has also focused on companies' failure to adopt "reasonably available" security measures to limit access between networks, such as employing firewalls or otherwise isolating systems with sensitive personal information. *See, e.g.*, Complaint at 10, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012) [hereinafter Wyndham Worldwide Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf, *archived at* http://perma.cc/R8J4-G6JA; Dave & Buster's Complaint at 2; Genica Complaint at 2–3; TJX Cos. Complaint at 2.

Further, the FTC has considered "readily available" security measures to limit access to computer networks through wireless access points. *See, e.g.*, Dave & Buster's Complaint at 2; Complaint at 13, *In re* GeneLink, Inc., & foru™ Int'l Corp., No. C-4456 (F.T.C. May 8, 2014) [hereinafter GeneLink and foru™ Complaint], http://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf, *archived at* http://perma.cc/APU8-4UUQ; Life is Good Complaint at 2; TJX Cos. Complaint at 2.

FTC enforcement proceedings also reference failures to implement or follow a variety of other "well known" or "commonly accepted" security practices, including the use of a commonly used algorithm to screen out credit card numbers. *See, e.g.*, Complaint at 4–5, *In re* Compete, Inc., No. C-4384 (F.T.C. Feb. 20, 2013) [hereinafter Compete Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf, *archived at* http://perma.cc/2DW3-43CX; commonly accepted and well known secure programming practices, including practices described in guidance documentation for software manufactures and developers, Complaint at 2, *In re* HTC America, Inc., No. C-4406 (F.T.C. June 25, 2013) [hereinafter HTC America Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf, *archived at* http://perma.cc/Y4UB-WD7A; readily available security measures to prevent unauthorized access, including installing patches and critical updates to the company's network, LifeLock Complaint at 10; readily available, low-cost measures to address risks of a software program collecting sensitive information in an unauthorized manner,

> The amount and sensitivity of the information at issue, and the degree of risk to its security.[62]

[23] Though there cannot be a single, uniform set of specific safeguards that comprise a reasonable security program for every organization in every industry, common elements nevertheless emerge from the various information safeguard laws and standards. Based on review of information security laws and guidance contained in ISO 27002 and the NIST Cybersecurity Framework, a reasonable information security program should include the six elements discussed below, consistent with applicable legal requirements, the organization's obligations to third-parties, and the organization's strategic approach to risk.

Complaint at 4, *In re* Upromise, Inc., No. C-4351 (F.T.C. Mar. 27, 2012) [hereinafter Upromise Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf , *archived at* http://perma.cc/ZZ2G-XEWB; and commonly used safeguards for requiring strong user passwords, Wyndham Worldwide Complaint at 11.

[62] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(1) (2014) ("commensurate with the sensitivity of the information . . . .") (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); 12 C.F.R. pt. 748, app. A(III)(C)(1) (2014) ("commensurate with the sensitivity of information . . . .") (NCUA Guidelines for Safeguarding Member Information under Gramm-Leach-Bliley); 16 C.F.R. § 314.3(a) (2014) ("appropriate to . . . the sensitivity of any customer information at issue.") (FTC Safeguards Rule under Gramm-Leach-Bliley); 45 C.F.R. § 164.306(b)(2)(iv) (2013) ("[t]he probability and criticality of potential risks to electronic protected health information.") (HIPAA Security Rule); 201 MASS. CODE REGS. 17.03(1) (2013) (appropriate to "the amount of stored data; and the need for security and confidentiality of both consumer and employee information.") (Massachusetts Standards for Protection of PII); OR. REV. STAT. § 646A.622(4) (West 2011) ("appropriate to . . . the sensitivity of the personal information collected from or about consumers [by the small business].") (Oregon PII Safeguards Statute).

A. Identify

An Organization Should Identify the Types of Information in Its Possession, Custody, or Control for Which It Will Establish Security Safeguards ("Protected Information")

[24] To establish a reasonable information security program, an organization should begin by identifying the types of information for which it will implement security safeguards. In so doing, the organization should consider applicable legal requirements to such safeguards, the organization's information security obligations to third-parties, and the organization's strategic approach to risk management.[63]

1. Information with Legally Required Safeguards

[25] In the United States, a mosaic of legal requirements mandate security for different types of regulated information.[64] Organizations

[63] The FTC has published guidance on data security in *Protecting Personal Information: A Guide for Business.* Federal Trade Comm'n, *Protecting Personal Information: A Guide for Business*, BUREAU OF CONSUMER PROTECTION BUSINESS CENTER (2011), *available at* http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business [hereinafter FTC Business Guidance]. The first of the FTC's five guidance principles, "Take Stock," is "[k]now what personal information you have in your files and on your computers." *Id.* at 3, 5.

[64] Beyond the legal requirements for information safeguards discussed in this section, a wide variety of laws simply require that specified types of information be kept confidential or must not be disclosed, without addressing the means by which that result must be accomplished. For example, under the Family Educational Rights and Privacy Act (FERPA), personally identifiable information in education records may not be released or accessed without consent or proper authorization. *See, e.g.*, 20 U.S.C. § 1232g(b)(1) (2012); 34 C.F.R. § 99.30 (2013) (FERPA disclosure regulations).

Employee medical records must be maintained confidentially by employers pursuant to regulations under various statutes applicable to the workplace. *See* 29 C.F.R. § 825.500(g) (2013) (covering the Family Medical Leave Act (FMLA)); 29 C.F.R. § 1630.14(b)–(d) (2013) (the Americans With Disabilities Act (ADA)); 29 C.F.R. § 1635.9(a)(1) (2013) (the Genetic Information Nondiscrimination Act (GINA)).

should determine what information they are must safeguard under these explicit legal requirements.

a. HIPAA PHI

[26] Under the HIPAA Security Rule, covered entities and business associates must safeguard electronic protected health information ("ePHI") of the covered entity.[65] PHI is individually identifiable health information, which (1) "[i]s created or received by a health care provider, health plan, employer, or health care clearinghouse;" (2) relates to the individual's physical or mental health, the provision of health care to the individual, or payment for providing such health care; and (3) either identifies the individual or reasonably could be used to identify the individual.[66]

[27] HIPAA's Security Rule applies only to HIPAA covered entities and business associates.[67] Covered entities include health plans, health care clearing houses, and health care providers who transmit health information electronically in HIPAA covered transactions, such as reimbursement.[68] Business associates are generally third-parties that

Occupational Safety and Health Administration regulations require confidentiality of employee names and personally identifiable information in certain disclosures of workplace injury and illness reporting, 29 C.F.R. § 1904.29(b)(10) (2013), and confidentiality for privacy concern case numbers and employee names, 29 C.F.R. § 1904.29(b)(6) (2013).

[65] *See* 45 C.F.R. § 164.302 (2013).

[66] *See* 45 C.F.R. § 160.103 (2013) (defining "*protected health information* and *individually identifiable health information*"). Electronic PHI is PHI that is transmitted by or maintained in electronic media. *See id.* (defining "*electronic protected health information*").

[67] *See* 45 C.F.R. § 164.302 (2013).

[68] *See* 45 C.F.R. § 160.103 (2013) (defining "*covered entity*").

create, receive, maintain, or transmit PHI on behalf of a covered entity, or that provide services to or for a covered entity (including legal, actuarial, accounting, consulting, data aggregation, management, administration, or financial services) that involve disclosure of PHI to the third-party.[69] Additionally, if a subcontractor creates, receives, maintains, or transmits PHI on behalf of the business associate, the subcontractor will also have business associate status under HIPAA.[70]

[28] The applicability of HIPAA is not always intuitive. For example, individually identifiable health information held by an employer's self-insured health plan would be subject to HIPAA, but the same type of health information in the human resources files of a general employer would not be covered by HIPAA, because merely being an employer does not trigger HIPAA covered entity status.[71] This distinction exists even if the employer is itself a HIPAA covered entity because individually identifiable health information "[i]n employment records held by the covered entity in its role as employer" is excluded from the definition of PHI.[72]

[29] Unlike PHI held by an employer's self-insured health plan, similar medical records held by an employer's self-insured worker's compensation plan do not trigger HIPAA security requirements, because workers' compensation and other liability insurance is excluded from the definition of a HIPAA covered health plan.[73]

[69] *See* 45 C.F.R. § 160.103 (2013) (defining "*business associate*").

[70] *See* 45 C.F.R. § 160.103 (2013).

[71] *See* 45 C.F.R. § 160.103 (defining "*covered entity*").

[72] *See id.* (defining "*protected health information*").

[73] *See, e.g.*, 45 C.F.R. § 160.103 (2013) (defining "*health plan*" as excluding plans providing for excepted benefits under 42 U.S.C. § 300gg-91(c)(1)); 42 U.S.C. § 300gg-91(c)(1) (2012) (excepting different categories of benefits, including liability insurance, workers' compensation, or similar insurance).

[30] Non-health care businesses, such as cloud service providers, banks, and law firms are nevertheless subject to HIPAA as business associates if they receive or maintain a covered entity's PHI.[74]

[31] Though the HIPAA Security Rule is limited to electronic PHI, covered entities and business associates must also safeguard PHI in paper media to avoid violating the HIPAA Privacy Rule.[75] For example, after Parkview Health System employees returned seventy-one cardboard boxes of paper medical records to a retired physician by leaving them unattended on the physician's home driveway, the resulting investigation conducted by the U.S. Department of Health and Human Services' Office of Civil Rights resulted in an $800,000 resolution payment and corrective action plan for Parkview; in light of Parkview having violated the HIPAA Privacy Rules' requirement to safeguard PHI.[76]

b. Gramm-Leach-Bliley Customer Information

[32] Under the Gramm-Leach-Bliley Act, financial institutions must protect the security and confidentiality of their customers' nonpublic personal information,[77] which is "personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution."[78] Gramm-

[74] *See* 45 C.F.R. § 160.103 (2013) (defining "*business associate*").

[75] *See* 45 C.F.R. § 164.502(a) (2013).

[76] *See, e.g.*, Press Release, U.S. Dep't of Health & Human Servs., $800,000 HIPAA Settlement in Medical Records Dumping Case (June 23, 2014), *available at* http://www.hhs.gov/news/press/2014pres/06/20140623a.html, *archived at* http://perma.cc/Z7NL-9C3P.

[77] *See* 15 U.S.C. § 6801(a) (2012).

[78] 15 U.S.C. § 6809(4) (2012).

Leach-Bliley contains the related but distinct terms "consumer" and "customer." Consumers are individuals who "obtain[], from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes . . . ." [79] Customer relationships are defined by the regulations promulgated under the Gramm-Leach-Bliley Act.[80] Thus, under the FTC regulations, customers are consumers who have a continuing relationship with a financial institution that "provide[s] one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes".[81]

[33] Financial institutions covered by Gramm-Leach-Bliley generally include any institution in the business of engaging in financial activities under the Bank Holding Company Act, including institutions engaged in activities that are a "proper incident" to banking under Federal Reserve Board regulation.[82]

c. FACTA Consumer Information

[34] Disposal Rule regulations promulgated under FACTA require proper disposal of consumer information and compilations of "consumer information, derived from consumer reports for a business purpose . . . ."[83]

[79] 15 U.S.C. § 6809(9) (2012).

[80] *See* 15 U.S.C. § 6809(11) (2012).

[81] 16 C.F.R. § 313.3(h)(i)(1) (2014).

[82] *See* 12 U.S.C. § 1843(k)(4)(F) (2012) (Bank Holding Company Act); 12 C.F.R. § 225.28 (2014) (Federal Reserve Board regulation). The Federal Trade Commission regulations contain further specific examples of financial institutions. *See, e.g.*, 16 C.F.R. § 313.3(k)(2) (2014).

[83] *See* 15 U.S.C. § 1681w(a)(1) (2012); *see also* 12 C.F.R. § 41.83(b) (2014); 12 C.F.R pt. 30, app. B(III)(C)(4) (2014); 12 C.F.R. § 222.83(b) (2014); 12 C.F.R. pt. 208, app. D-2(III)(C)(4) (2014); 12 C.F.R. § 334.83(a) (2014); 12 C.F.R. pt. 364, app. B(III)(C)(4)

Consumers are individuals,[84] and consumer reports include written communication of any information by a consumer reporting agency bearing on a consumer's credit, "character, general reputation, personal characteristics, or mode of living," to be used or collected as "a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, employment purposes; or any other [specified] purpose[s]."[85]

d. COPPA Online Personal Information

[35] Regulations under COPPA require safeguards for personal information that covered websites or online services collect from children.[86] Children are individuals under the age of thirteen,[87] and personal information is individually identifiable information collected online that

> [I]nclud[es] a first and last name; a home or other physical address including street name and name of city or town; an e-mail address; a telephone number; a Social Security number; . . . or information concerning the child or the parents of that child that the website collects online from the child and combines with [any specified] identifier; [or] any other identifier that the [Federal Trade] Commission determines permits the physical or online contacting of a specific [child].[88]

(2014); 12 C.F.R. § 717.83(a) (2014); 12 C.F.R. pt. 748, app. A(III)(C)(4) (2014); 16 C.F.R. § 682.3(a) (2014); 17 C.F.R. § 248.30(b)(2) (2014).

[84] *See* 15 U.S.C. § 1681a(c) (2012).

[85] *See* 15 U.S.C. § 1681a(d)(1)(A)–(C) (2012).

[86] *See* 15 U.S.C. § 6502(b)(1)(D) (2012).

[87] *See* 15 U.S.C. § 6501(1) (2012).

e. State-Level PII

[36] Virtually every state (except Alabama, New Mexico, and South Dakota) requires persons or organizations possessing PII of their residents to notify residents of security breaches concerning their PII.[89] Several states affirmatively require reasonable security procedures and practices to protect resident's PII, and others require either a destruction policy or secure means of disposal for such PII.[90] These laws generally apply to PII in computerized form, but at least nine jurisdictions apply some or all of their safeguards and notification requirements to PII in both computerized and hard copy form.[91] Effective encryption of electronic PII is generally a safe harbor for breach notification obligations.[92]

---

[88] *See* 15 U.S.C. § 6501(8) (2012). FTC regulations add additional identifiers, including online contact information as defined in the regulations; screen or user names that function in the same manner as online contact information; persistent identifiers that can be used to recognize users over time and across different websites or online services, such as customer numbers held in a cookie, IP addresses, processor or device serial numbers, or unique device identifiers; photograph, video, or audio files containing a child's image or voice; and geolocation information sufficient to identify street and city or town names. *See* 16 C.F.R. § 312.2 (2014) (defining "*personal information*").

[89] *See, e.g.*, GINA STEVENS, CONG. RESEARCH SERV., R42475, DATA SECURITY BREACH NOTIFICATION LAWS 4 (2012) (citation omitted). In 2014, Kentucky became the forty-seventh state to enact a breach notification law. *See* KY. REV. STAT. ANN. § 365.732(2) (LexisNexis Supp. 2014). Puerto Rico, Guam, and the U.S. Virgin Islands also have PII breach notification requirements. *See* P.R. LAWS ANN. tit. 10, § 4052 (2012); 9 GUAM CODE ANN. § 48.30(a) (2013); V.I. CODE ANN. tit. 14, § 2209(a) (2013).

[90] *See infra* notes 282–99.

[91] *See, e.g.*, ALASKA STAT. § 45.48.090(7) (2012); ARK. CODE ANN. § 4-110-103(5) (Supp. 2011) (medical information only); HAW. REV. STAT. ANN. § 487N-1 (LexisNexis Supp. 2012); IND. CODE ANN. § 24-4.9-2-2(a) (2013); MASS. GEN. LAWS ch. 93H, § 1(a) (2012); N.C. GEN. STAT. §§ 75-61(12), (14) (2013); P.R. LAWS ANN. tit. 10, § 4051(a) (2012); S.C. CODE ANN. § 39-1-90(A) (Supp. 2013); WIS. STAT. § 134.98(1)(c)(1) (2012).

[92] *See, e.g.*, VA. CODE ANN. § 18.2-186.6(A) (Supp. 2014).

[37] The several states commonly define PII as a combination of the resident's name and any information in additional categories, such as the resident's Social Security number, driver's or state identification number, or financial account or card numbers with account access information—such as security or access codes or PINs.[93] However, some states add additional categories of combined information, including medical information (Arkansas, California, Florida, Missouri, Puerto Rico, and Texas);[94] health insurance information (California, Florida, Missouri, North Dakota, and Texas);[95] unique biometric data or DNA profiles (Iowa, Nebraska, North Carolina, Texas, and Wisconsin);[96] taxpayer identification numbers or other tax information (Maryland and Puerto Rico);[97] digital signatures (North Carolina, North Dakota, and Texas);[98] electronic identification numbers, e-mail names or addresses, and Internet account numbers or identification names (Florida and North Carolina);[99]

[93] *See, e.g.*, § 18.2-186.6(A).

[94] *See* ARK. CODE ANN. § 4-110-103(7)(D) (Supp. 2011); CAL. CIV. CODE § 1798.82(h) (Deering 2005); FLA. STAT. ANN. § 501.171(1)(g)(1) (2014); MO. REV. STAT. § 407.1500.1(9)(e)–(f) (Supp. 2011); P.R. LAWS ANN. tit. 10, § 4051(a)(5) (2012); TEX. BUS. & COM. CODE ANN. § 521.002(a)(2)(B) (West 2009 & Supp. 2014).

[95] *See* CAL. CIV. CODE § 1798.82(h) (Deering 2005); FLA. STAT. ANN. § 501.171(1)(g)(1) (2014); MO. REV. STAT. § 407.1500.1(9)(f) (Supp. 2011); N.D. CENT. CODE § 51-30-01(4)(a)(8) (2007 & Supp. 2013); TEX. BUS. & COM. CODE ANN. § 521.002(a)(2) (West 2009 & Supp. 2014).

[96] *See* IOWA CODE § 715C.1(11)(e) (2013); NEB. REV. STAT. § 87-802(5)(e) (2008); N.C. GEN. STAT. §§ 14-113.20(b)(11)–(12), 75-61(10) (2013); TEX. BUS. & COM. CODE ANN. § 521.002(a)(1)(C) (West 2009 & Supp. 2014); WIS. STAT. § 134.98(1)(b)(4)–(5) (2012).

[97] *See* MD. CODE ANN., COM. LAW § 14-3501(d)(1)(iv) (LexisNexis Supp. 2013); P.R. LAWS ANN. tit. 10, § 4051(a)(6) (2012).

[98] *See* N.C. GEN. STAT. §§ 14-113.20(b)(9), 75–61(10) (2013); N.D. CENT. CODE § 51-30-01(4)(a)(10) (2007 & Supp. 2013); TEX. BUS. & COM. CODE ANN. § 521.002(a)(1)(D) (West 2009 & Supp. 2014).

employment identification numbers (North Dakota);[100] birth dates (North Dakota and Texas);[101] parents' surnames before marriage, such as maiden names (North Carolina, North Dakota, and Texas);[102] and work-related evaluations (Puerto Rico).[103] Georgia and Maine provide that information in their combination categories can constitute protected PII in the absence of the resident's name if such information would sufficiently enable identity theft.[104] In Florida, a user name or e-mail address combined with a password or security question and answer, permitting access to an online account, is protected PII even without the resident's name.[105]

f. FTC Act Section 5 Protected Information

[38] In FTC enforcement actions under Section 5 of the FTC Act, not involving enforcement of Gramm-Leach-Bliley, FACTA, or COPPA, the most common type of protected information is nonpublic personal information conducive to identity theft, including consumer names, physical and e-mail addresses and telephone numbers, Social Security numbers, purchase card numbers, card expiration dates and security codes, financial account numbers, and driver's license or other government-

[99] *See* FLA. STAT. ANN. § 501.171(1)(g)(1)(b) (2014); N.C. GEN. STAT. §§ 14-113.20(b)(8), 75-61(10) (2013).

[100] *See* N.D. CENT. CODE § 51-30-01(4)(a)(9) (2007 & Supp. 2013).

[101] *See* § 51-30-01(4)(a)(5); TEX. BUS. & COM. CODE ANN. § 521.002(a)(1)(A) (West 2009 & Supp. 2014).

[102] *See* N.C. GEN. STAT. §§ 14-113.20(b)(14), 75-61(10) (2013); N.D. CENT. CODE § 51-30-01(4)(a)(6) (2007 & Supp. 2013); TEX. BUS. & COM. CODE ANN. § 521.002(a)(1)(B) (West 2009 & Supp. 2014).

[103] *See* P.R. LAWS ANN. tit. 10, § 4051(a)(7) (2012).

[104] *See* GA. CODE ANN. § 10-1-911(6)(E) (2009); ME. REV. STAT. tit. 10, § 1347(6)(E) (Supp. 2013).

[105] *See* FLA. STAT. ANN. § 501.171(1)(g)(1)(b) (2014).

issued identification numbers.[106] These categories of information are familiar territory under state laws protecting PII. In Section 5 enforcement actions against healthcare-related entities, the FTC has also treated additional categories of nonpublic personal information as requiring safeguards, including patient names with billing information and diagnostic information;[107] physician names, insurance numbers, diagnosis codes, and medical visit types;[108] medical record numbers, healthcare provider names, addresses, and phone numbers, lab tests and test codes, lab results and diagnoses, clinical histories, and health insurance company names and policy numbers;[109] prescription medications and dosages,

[106] *See, e.g.*, Accretive Health Complaint at 2; *see also* Wyndham Worldwide Complaint at 7; ValueClick Complaint at 9–10; BJ's Wholesale Club Complaint at 2–3; Cardsystems Solutions Complaint at 1, 3; Cbr Systems Complaint at 1–2, 4; Ceridian Corp. Complaint at 2–3; Compete Complaint at 1, 3, 7; Credit Karma Complaint at 1–2, 6; Complaint at 2–3, CVS Caremark Corp., No. C-4259 (F.T.C. June 23, 2009), [hereinafter CVS Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf, *archived at* http://perma.cc/P3V3-JUQJ; Dave & Buster's Complaint at 2; DSW Complaint at 1, 3; EPN Complaint at 1, 3; Fandango Complaint at 2, 4–5; GeneLink and foru™ Complaint at 12, 14; Genica Complaint at 2–3; Guess Complaint at 1–2; Complaint at 2, 4, GMR Transcription Services, Inc., No. 122-3095 (F.T.C. Jan. 31, 2014) [hereinafter GMR Transcription Services Complaint], http://www.ftc.gov/system/files/documents/cases/140203gmrcmpt.pdf, *archived at* http://perma.cc/9R58-EYJF; Guidance Software Complaint at 1; LabMD Complaint at 2; Complaint at 1, Lookout Services, Inc., No. C-4326, (F.T.C. June 15, 2011), [hereinafter Lookout Services Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110615lookoutcmpt.pdf, *archived at* http://perma.cc/5SF5-EC6N; Life is Good Complaint, at 2; LifeLock Complaint at 4–5; Petco Complaint at 1, 4; Complaint at 1–3, Rite Aid Corp., No. C-4308 (F.T.C. Nov. 22, 2010), [hereinafter Rite Aid Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaidcmpt.pdf, *archived at* http://perma.cc/FB2Q-V6TJ; TJX Complaint at 2–3; Upromise Complaint at 3, 6.

[107] *See* Accretive Health Complaint at 2.

[108] *See* EPN Complaint at 1.

[109] *See* LabMD Complaint at 2.

prescribing physician names, addresses, and telephone numbers, health insurer names, and insurance account and policy numbers;[110] genetic information;[111] medical histories, health care providers' examination notes, medications, and psychiatric notes;[112] and medical health history profiles, blood type results, infectious disease marker results, newborn children's names, genders, birth dates and times, birth weights, delivery types, and adoption types (open, closed, or surrogate).[113] These categories of health-related personal information are comparable to HIPAA-protected PHI. Other FTC enforcement actions under Section 5 have focused on safeguards for nonpublic consumer identification information from credit reporting agencies[114] and credit report information generally;[115] information similar to that protected under FACTA.

[39] Several FTC Section 5 enforcement proceedings under a deception theory have focused on safeguards for the security of consumers' online activity information, such as data on consumers' user names, passwords, search terms, websites visited, links followed, ads viewed, and shopping cart actions;[116] nonpublic social network profile information;[117] and nonpublic smart phone data, including text message content, GPS location

[110] *See* CVS Complaint at 2; *see also* Rite Aid Complaint at 1–2.

[111] *See* GeneLink and foru™ Complaint at 12.

[112] *See, e.g.*, GMR Transcription Services Complaint at 2.

[113] *See, e.g.*, Cbr Systems Complaint at 1–2.

[114] *See, e.g.*, Reed Elsevier Complaint at 2.

[115] *See, e.g.*, Credit Karma Complaint at 1–2.

[116] *See, e.g.*, Compete Complaint at 3; *see also* Upromise Complaint at 2.

[117] *See, e.g.*, Complaint at 2–3, Facebook, Inc., No. C-4365, (F.T.C. Aug. 10, 2012) [hereinafter Facebook Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf , *archived at* http://perma.cc/47BF-9VV3; *see also* Myspace Complaint at 1–2; Twitter Complaint at 1–2.

data, web browsing and media viewing history, phone numbers of users and contacts, and numeric keys pressed.[118] Most of this information is well beyond what traditionally comprises PII under state statutes, but in each of the above matters the FTC alleged that the subject company engaged in deceptive conduct by misrepresenting that the information would remain private or be safeguarded.[119]

[40] The FTC, using Section 5 deceptive theory, has also pursued data security enforcement actions against retailers for failure to safeguard personal information beyond traditional PII, including shipping addresses, order numbers, and information on all previously purchased products, in alleged violation of the companies' privacy policies.[120]

[41] In its enforcement action against Eli Lily, the FTC's Section 5 deception claim simply focused on the names and e-mail addresses contained within a single group e-mail sent to 669 persons.[121] The additional factors were that the recipients were subscribers to a "MEDI-messenger" service of the manufacturer of Prozac, and the disclosure of their identities was alleged to violate the applicable privacy policy.[122]

[42] In the matter of *TRENDnet, Inc.*, an FTC information security enforcement matter based on both deception and unfairness under Section 5, the protected information was live video feed images from Internet Protocol (IP) cameras used by TRENDnet's customers for business and home monitoring.[123] Notably, live video feeds are not specified as

[118] *See, e.g.*, HTC America Complaint at 5.

[119] *See* text accompanying *supra* notes 116–18.

[120] *See, e.g.*, MTS and Tower Direct Complaint at 2; *see also* ValueClick Complaint at 9–10.

[121] *See* Eli Lily Complaint at 3.

[122] *See id.*

protected information under any identified federal or state data security statute or regulation. The FTC's claim under the deceptive prong of Section 5 was based on alleged misrepresentations in TRENDnet's marketing and sales materials.[124] In support of its unfairness allegations, the FTC stated:

> The exposure of sensitive information through respondent's IP cameras increases the likelihood that consumers or their property will be targeted for theft or other criminal activity, increases the likelihood that consumers' personal activities and conversations or those of their family members, including young children, will be observed and recorded by strangers over the Internet. This risk impairs consumers' peaceful enjoyment of their homes, increases consumers' susceptibility to physical tracking or stalking, and reduces customers' ability to control the dissemination of personal or proprietary information (*e.g.*, intimate video and audio feeds or images and conversations from business properties). Consumers had little, if any, reason to know that their information was at risk, particularly those consumers who maintained login credentials for their cameras or who were merely unwitting third parties present in locations under surveillance by the cameras.[125]

[123] *See* Complaint at 5, TRENDnet, Inc., No. C-4426, (F.T.C. Feb. 7, 2014) [hereinafter TRENDnet Complaint], http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf, *archived at* http://perma.cc/QQG3-Q9X7.

[124] *See id.* at 3–4.

[125] *Id.* at 6.

2. Information Protected Due to Third-Party Obligations

[43] Organizations may have contractual obligations to safeguard certain types of information. For example, organizations that are service providers or suppliers to other entities may be required by contract to have certain safeguards in place for protected information.[126] And companies that store, process, or transmit payment card information may by contract be subject to the Payment Card Industry (PCI) Data Security Standard, which sets forth extensive, detailed security safeguards and controls for cardholder data.[127] Organizations should therefore consider their contractual obligations when identifying the types of information to which they will apply security safeguards.

[126] *See* text accompanying *infra* notes 282–83, 285, 293–99.

[127] *See* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES 5 (Version 2.0 ed. 2010) [hereinafter PCI 2.0], *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf, *archived at* http://perma.cc/PDY8-XG3G. The PCI Data Security Standard provides technical and operational requirements to protect cardholder data, and it "applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data." *Id.* at 5. While Version 2.0 of PCI DSS remains active until December 31, 2014, Version 3.0 was issued in November 2013 by the PCI Security Standards Council to allow organizations time to adjust their practices for compliance with the revised requirements. *See* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD AND PAYMENT APPLICATION DATA SECURITY STANDARD: VERSION 3.0 CHANGE HIGHLIGHTS, at 1 (2013) *available at* https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf, *archived at* http://perma.cc/A5MT-L62C.

3. Information Protected Consistent with the Organization's Risk Strategy

[44] There may be other categories of information for which the organization will choose to apply safeguards to preserve confidentiality, such as nonpublic, strategic business information. As noted above, if the organization wants to enjoy trade secret protection for certain confidential business information it must take reasonable measures to maintain the information's secrecy.[128] Regardless of whether legally protectable trade secret status exists, most organizations will want to maintain an appropriate level of confidentiality regarding information they have assembled for a business or operational advantage.

[45] If an organization voluntarily chooses to participate in the U.S.-EU Safe Harbor Program, it will be obligated to abide by the Safe Harbor Privacy Principles, including the Security Principle, under which the organization must take reasonable precautions to protect personal information.[129] Such organizations should therefore identify personal data protected under the Safe Harbor and other data protection laws of European Union countries involved in this directive.[130]

[46] ISO 27002 highlights the importance of identifying information that must be safeguarded in compliance with legal and contractual requirements.[131] Such controls include identification of applicable legislation and contractual requirements regarding safeguards generally,

[128] *See* 18 U.S.C. § 1839(3)(a) (2012) ("the owner therefore has taken reasonable measures to keep such information secret"); *see also* UNIF. TRADE SECRETS ACT § 1(4)(ii) (1985) ("is the subject of efforts that are reasonable under the circumstances to maintain its secrecy").

[129] *See U.S.-EU Safe Harbor Overview*, EXPORT, http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last visited Oct. 1, 2014), *archived at* http://perma.cc/LVY2-GRKG.

[130] *See id.*

[131] *See* ISO 27002, *supra* note 5, at § 18.1.1 (2013).

intellectual property rights, protection of records, privacy and protection of personally identifiable information, and cryptographic controls.[132] ISO 27002 also provides guidance on controls for information classification, including controls for information classification, labeling of information, and handling of assets.[133]

[47] The NIST Cybersecurity Framework, under its Identify function, provides a range of activities in the category of Asset Management, under which "[t]he data . . . that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy."[134] These activities include identifying data and the related physical devices, systems, software platforms, and applications, mapping data flows, and prioritizing based on classification, criticality, and business value.[135]

B. Assess

An Organization Should Assess Anticipated Threats, Vulnerabilities, and Risks to the Security of Protected Information

[48] Once it determines the types of information to be safeguarded, an organization should then assess anticipated threats, vulnerabilities, and risks to the security of that information. Such an assessment is crucial to

[132] *See id.* at §18.1.

[133] *See id.* at § 8.2.

[134] Nat'l Inst. Of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity 20 (Version 1.0, 2014) [hereinafter Cybersecurity Framework] *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, *archived at* http://perma.cc/U23X-MV6S.

[135] *See id.*

help the organization understand its information security environment and to identify its priorities in developing an information security program.

[49] Various laws mandate assessments of information security threats, vulnerabilities, and risks. HIPAA covered entities and business associates must "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate." [136] The interagency guidelines establishing information security standards under Gramm-Leach-Bliley require risk assessment as well. Banks must:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.[137]

[50] The FTC Safeguards Rule under Gramm-Leach-Bliley similarly requires a risk assessment to "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse,

[136] 45 C.F.R. § 164.308(a)(1)(ii)(A) (2013).

[137] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(B) (2014) (OCC); 12 C.F.R. pt. 170, app. B(III)(B) (2014) (OCC); 12 C.F.R. pt. 208, app. D-2(III)(B) (2014) (Federal Reserve Board); 12 C.F.R. pt. 225, app. F(III)(B) (2014) (Federal Reserve Board); 12 C.F.R. pt. 364, app. B(III)(B) (2014) (FDIC); *see also* 12 C.F.R. pt. 748, app. A(III)(B) (2014) (NCUA).

alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks."[138] The FTC Safeguards Rule further provides:

> At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including: (1) Employee training and management; (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.[139]

[51] In its PII Protection Standards, Massachusetts requires persons that own or license PII of Massachusetts' residents to have a comprehensive information security program that includes "[i]dentifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information . . . ."[140] Under the Massachusetts Standards, such an assessment must be focused on "evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: (1) ongoing employee (including temporary and contract employee) training; (2) employee compliance with policies and procedures; and (3) means for detecting and preventing security system failures."[141] Oregon's statute requiring safeguards for PII sets forth elements of a security program that shall be deemed compliant, including identifying "reasonably foreseeable internal

[138] 16 C.F.R. § 314.4(b) (2014).

[139] *Id.*

[140] 201 MASS. CODE REGS. 17.03(2)(b) (2014).

[141] *Id.*

and external risks" and assessing "the sufficiency of safeguards in place to control the identified risks."[142]

[52] FTC enforcement actions under the authority of Gramm-Leach-Bliley commonly allege a failure to "identify reasonably foreseeable internal and external risks to customer information."[143] The FTC has also taken the position in enforcement actions under the authority of Section 5 of the FTC Act that the failure to "perform assessments to identify reasonably foreseeable risks to the security, integrity, and confidentiality of consumers' personal information" may constitute an unfair or deceptive trade practice.[144] Additionally, FTC consent orders routinely require that

[142] OR. REV. STAT. ANN. § 646A.622(2)(d)(A)(ii)(iii) (West 2011).

[143] *See, e.g.*, Complaint at 2–3, United States v. American United Mortg. Co., No. 07C-7064 (N.D. Ill. Dec. 17, 2007) [hereinafter American United Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2007/12/071217americanunitedmrtgcmplt.pdf, *archived at* http://perma.cc/UNS3-W6Z9; *see also* Complaint at 2, Goal Financial, LLC, No. C-4216 (F.T.C. Apr. 15, 2008) [hereinafter Goal Financial Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2008/04/080415complaint_0.pdf, *archived at* http://perma.cc/4P5C-TC4X; Complaint at 3, James B. Nutter & Co., No. C-4258 (F.T.C. May 5, 2009) [hereinafter James B. Nutter & Co. Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090616nuttercmpt.pdf, *archived at* http://perma.cc/DQ9T-J2HJ; Nations Title Agency Complaint at 3; Complaint at 2, Nationwide Mortg. Grp., Inc., No. 9319 (F.T.C. Nov. 9, 2004) [hereinafter Nationwide Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2004/11/041116cmp0423104.pdf, *archived at* http://perma.cc/EG9Q-WDC5; Complaint at 4, Premier Capital Lending, Inc., No. C-4241 (F.T.C. Nov. 6, 2008) [hereinafter Premier Capital Lending Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2008/11/081106pclcmpt.pdf, *archived at* http://perma.cc/754L-P4F5; Complaint at 4, SettlementOne Credit Corp., No. C-4330 (F.T.C. Aug. 17, 2011) [hereinafter SettlementOne Credit Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonecmpt.pdf, *archived at* http://perma.cc/D9HG-ZC2L; and Complaint at 2, Sunbelt Lending Servs., Inc., No. C-4129 (F.T.C. Nov. 16, 2004) [hereinafter Sunbelt Lending Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2004/11/041116cmp0423153.pdf, *archived at* http://perma.cc/LMC6-SPKR.

the respondent company "[identify] material internal and external risks to the security, confidentiality and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and the assessment of the sufficiency of any safeguards in place to control the risks."[145]

[53] ISO 27002 does not provide methodologies for assessment of security risks, as it is instead a compendium of controls to be adopted and applied to address identified risks.[146] Risk assessment is more directly addressed in a companion standard, ISO 27005, which deals with information security risk management.[147]

[54] The NIST Cybersecurity Framework provides a useful structure for risk assessment and development of a risk management strategy. Through risk assessment, "[t]he organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals."[148] In risk assessment:

---

[144] *See* GeneLink and foru™ Complaint at 13; *see also* LabMD Complaint at 3 (respondent "did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities of its networks.").

[145] *See* Accretive Health Order at 3. *See generally, e.g.*, RockYou Order at 5, 8 (example of consent orders under COPPA); ACRAnet Order at 2–3 (example of consent orders under the Gramm-Leach-Bliley Security Rule); Cbr Systems Order at 3 (example of consent orders under FTC Act §5).

[146] *See* ISO 27002, *supra* note 5, at § 0.2(a) (One means to identify an organization's security requirements is "the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated").

[147] *See* INT'L ORG. FOR STANDARDIZATION, ISO 27005, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—INFORMATION SECURITY RISK MANAGEMENT at 6–9, (2011) [hereinafter ISO 27005].

[148] Cybersecurity Framework, *supra* note 134, at 22.

> Asset vulnerabilities are identified and documented; . . . [t]hreat and vulnerability information is received from information sharing forums and sources; . . . [t]hreats, both internal and external, are identified and documented; . . . [p]otential business impacts and likelihoods are identified; . . . [t]hreats, vulnerabilities, likelihoods, and impacts are used to determine risk; [and] . . . [r]isk responses are identified and prioritized.[149]

Then, through development of a risk management strategy, "[t]he organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions." [150] In developing a risk management strategy, "[r]isk management processes are established, managed, and agreed to by organizational stakeholders; . . . [o]rganizational risk tolerance is determined and clearly expressed; [and] . . . [t]he organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis."[151]

C. Safeguard

An Organization Should Establish and Maintain Appropriate Policies and Administrative, Physical, and Technical Controls to Address the Identified Threats, Vulnerabilities, and Risks to the Security of Protected Information

[55] Informed by its risk assessment regarding the types of information to be safeguarded, an organization should establish and maintain appropriate policies and controls to address the identified threats,

[149] *Id.* at 22–23.

[150] *Id.* at 23.

[151] *Id.*

vulnerabilities, and risks to the security of such information.[152] The policy and controls selected should be consistent with applicable legal requirements, the organization's information safeguards obligations to third-parties, and its strategic approach to risk management. As discussed below, the program should also address training and awareness for employees and others with access to protected information. Moreover, the effectiveness of the selected safeguards should be tested or otherwise evaluated, to provide reasonable assurance that the organization's objectives for information security will be met.

1. Information Security Policy

[56] An organization should have a policy or policies that address what categories of information will be subject to security safeguards, how such safeguarding will be accomplished, and who or what functions within the organization have what responsibilities in that regard. Legal requirements for information security commonly require a written information security program to address identified risks.[153] Several such laws require a

[152] FTC Consent Orders commonly require "[t]he design and implementation of reasonable safeguards to control the risks identified through risk assessment . . . ." *See* Accretive Health Order at 3; s*ee also supra* note 145 and accompanying text.

[153] *See, e.g.*, 12 C.F.R. pt. 30, app. B(II)(A) (2014) ("[e]ach bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards . . . .") (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); 16 C.F.R. § 314.3(a) (2014) ("[y]ou shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts . . . .") (FTC Safeguards Rule under Gramm-Leach-Bliley); 45 C.F.R. § 164.308(a)(1)(i) (2013) ("[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."), 45 C.F.R. § 164.316(a) (2013) ("[i]mplement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart . . . ."); 45 C.F.R. § 164.316(b)(1) (2013) ("[m]aintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form . . . .") (HIPAA Security Rule); 201 MASS. CODE REGS. 17.03(1) (2013) ("develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards . . . .") (Massachusetts PII Protection

designation of who is responsible for implementing and maintaining the program.[154]

[57] In its enforcement proceedings under Gramm-Leach-Bliley and FACTA, the FTC has frequently focused on the respondent's failure to develop a comprehensive written information security program.[155] The FTC has also taken the position in enforcement proceedings under Section 5 of the FTC Act that the failure to "implement reasonable policies and procedures to protect the security of consumers' personal information

Standards); OR. REV. STAT. ANN. § 646A.622(2)(d) (West 2011) ("[a] person that implements an information security program" including specified features will be deemed in compliance) (Oregon PII Safeguards statute).

[154] The interagency guidelines establishing information security standards under Gramm-Leach-Bliley require that the board of directors or an appropriate board committee must approve the written information security program and "[o]versee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management." *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(A) (2014). Annual reporting to the board or an appropriate board committee on compliance and the overall status of the information security program is also required. *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(F).

Organizations subject to the FTC Safeguards Rule must "[d]esginate an employee or employees to coordinate [the] information security program." *See, e.g.*, 16 C.F.R. § 314.4(a) (2014). The HIPAA Security Rule requires covered entities and business associates to "[i]dentify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart . . . ." 45 C.F.R. § 164.308(a)(2) (2014).

Organizations subject to the Massachusetts PII Protection Standards must "[designate] one or more employees to maintain the comprehensive information security program . . . ." 201 MASS. CODE REGS. 17.03(2)(a). Organizations are deemed in compliance with the Oregon PII Safeguards Statute if, among other matters, they "[designate] one or more employees to coordinate the security program . . . ." OR. REV. STAT. ANN. § 646A.622(2)(d)(i) (West 2011).

[155] *See, e.g.*, American United Complaint at 3, 6; Goal Financial Complaint at 2–3; James B. Nutter & Co. Complaint at 2–3; Nations Title Agency Complaint at 3; Nationwide Complaint at 2–3; SettlementOne Credit Complaint at 4; *and* Sunbelt Lending Complaint at 2–3.

collected and maintained by respondents" is an unfair and deceptive trade practice,[156] and that the failure to "develop, implement, or maintain a comprehensive information security program to protect consumers' personal information" can also be an unfair trade practice.[157]

[58] As discussed previously, FTC Consent Orders under the authority of Gramm-Leach-Bliley, COPPA, and Section 5 of the FTC Act commonly require the respondent to establish a written, comprehensive information security program.[158] Such orders commonly also require "[t]he designation of an employee or employees to coordinate and be accountable for the information security program . . . ."[159]

[59] ISO 27002 provides that "[a] set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties."[160] "All information security responsibilities should be defined and allocated,"[161] and "[o]perating procedures should be documented and made available to all users who need them."[162]

[60] The NIST Cybersecurity Framework addresses security policies in its Governance category within the Identify function, in which an "[o]rganizational information security policy is established; [i]nformation security roles [and] responsibilities are coordinated and aligned with internal roles and external partners; [l]egal and regulatory requirements

[156] *See* GeneLink and foru™ Complaint at 13–14.

[157] *See, e.g.*, LabMD Complaint at 3.

[158] *See supra* notes 145 and accompanying text.

[159] *E.g.*, Accretive Health Order at 3.

[160] *See* ISO 27002, *supra* note 5, at § 5.1.1.

[161] *See id.* at § 6.1.1.

[162] *See id.* at § 12.1.1.

regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed; [and] . . . [g]overnance and risk management processes address cybersecurity risks."[163]

2. Controls

[61] An organization may appropriately establish a variety of administrative, physical, and technical controls to address its information security risks. As discussed above, different organizations in different industries and circumstances will have different security risks, and so the selection of appropriate controls will vary between organizations.[164] Below are eleven categories of security controls commonly referenced in information safeguards legal requirements and voluntary security standards, including controls for system access, physical access, encryption, transmission security, mobile device and portable media security, system change management, employee management, environmental risk, monitoring and detection, retention, and disposal.

a. System Access Controls

[62] System access controls are designed to help ensure that only authorized individuals have access to systems containing protected

[163] Cybersecurity Framework, *supra* note 134, at 21–22.

[164] The 2014 Verizon Data Security Report recommends safeguards priorities for each of its nine security incident patterns, which differ in frequency between industries. *See 2014 Verizon Data Security Report*, *supra* note 57 and accompanying text. For example, priority security controls for Point-of-Sale Attacks include remote access restrictions, strong password enforcement, limiting use of POS systems to their intended purpose, and effective anti-virus software. *See id.* at 19. In contrast, priority security controls for Physical Theft and Loss include device encryption, avoiding leaving devices unattended, regular backup, lock-down of equipment located in offices, and (believe it or not) the use of unappealing devices. *See id.* at 28.

information. These controls also commonly feature mechanisms to authenticate the identity of the individual seeking access.[165]

[63] System access controls are commonly required under legal requirements for information security programs,[166] and in its data security enforcement actions, the FTC frequently cites shortcomings in system access controls related to passwords or other user credentials, including: failure to use strong passwords;[167] failure to require periodic change of passwords or to prohibit use of the same password across multiple

[165] *See* FTC Business Guidance, *supra* note 63, at 9, 12–15 (addressing system access controls under principle 3 (Lock It) "protect the information that you keep," under Password Management, Firewalls, and Wireless and Remote Access).

[166] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(1)(a) (2014) (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); 16 C.F.R. § 314.4(b)–(c) (2014) (requirement to implement information safeguards to control identified risks, including the "unauthorized disclosure, misuse, alteration, destruction or other compromise" of protected information and the FTC Safeguards Rule under Gramm-Leach-Bliley); 45 C.F.R. § 164.308(a)(4)(i) (2013) (the HIPAA Security Rule requires "policies and procedures for authorizing access to electronic protected health information . . ."); 45 C.F.R. § 164.312(d) (2013) ("procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed"); 45 C.F.R. § 164.312(a)(1)–(2)(ii) (2013) (The HIPAA Security Rule also requires "technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights . . . ." including unique user identification and emergency access procedures); 45 C.F.R. § 164.308(a)(4)(ii)(B)–(C) (2013) (Addressable implementation specifications include access authorization and access establishment and modification); 45 C.F.R. § 164.308(a)(5)(ii)(C) (2013) ("[l]og-in monitoring"); 45 C.F.R. § 164.308(a)(5)(ii)(D) ("[p]assword management"); 45 C.F.R. § 164.312(a)(2)(iii) (2013) ("[a]utomatic logoff"); 45 C.F.R. § 164.312(a)(2)(iv) (2013) ("encryption"); *see also* 201 MASS. CODE REGS. 17.04(1),(2) (secure user authentication protocols and secure access control measures, Massachusetts PII Protection Standards); OR. REV. STAT. ANN. § 646A.622(2)(d)(C)(iii) (West 2011) (safeguards to protect against unauthorized access to personal information, Massachusetts PII Protection Statute).

[167] *See, e.g.*, CardSystems Solutions Complaint at 2; *see also* Wyndham Worldwide Complaint at 11–12; LifeLock Complaint at 10; Lookout Services Complaint at 2; Reed Elsevier Complaint at 3; TJX Complaint at 2; Twitter Complaint at 4.

applications and programs;[168] failure to suspend users after a reasonable number of unsuccessful login attempts;[169] and the practice of storing passwords or other network user credentials in clear readable text.[170] In at least two enforcement matters, the FTC has focused on a security flaw of allowing commonly known or used default user IDs and passwords, or the sharing of user credentials among a third-party's multiple users, thereby reducing the likelihood of detecting unauthorized access.[171] In other enforcement matters, the FTC has focused on additional shortcomings in system access safeguards, including the failure to restrict access between and among systems with firewalls;[172] the failure to use reasonable efforts to verify or authenticate the identity and qualifications of users, such as third-party subscribers, for accessing protected information;[173] and the

[168] *See, e.g.*, LabMD Complaint, at 3; *see also* LifeLock Complaint at 10; Lookout Services Complaint at 2; Reed Elsevier Complaint at 3; TJX Complaint at 2; Twitter Complaint at 4.

[169] *See, e.g.*, LifeLock Complaint at 10; *see also* Lookout Services Complaint at 2; Reed Elsevier Complaint at 3; Twitter Complaint at 4.

[170] *See, e.g.*, Guidance Software Complaint at 2; *see also* Reed Elsevier Complaint at 3; Twitter Complaint at 4.

[171] *See, e.g.*, BJ's Wholesale Club Complaint at 2; *see also* Reed Elsevier Complaint at 3.

[172] *See, e.g.*, Dave & Buster's Complaint at 2; *see also* Wyndham Worldwide Complaint at 10.

[173] *See, e.g.*, Complaint at 3, Equifax Info. Servs., LLC, No. C-4387 (F.T.C. Mar. 5, 2013) [hereinafter Equifax Complaint] http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121010equifaxcmpt.pdf, *archived at* http://perma.cc/4BWH-LKEM; *see also* Complaint at 9, United States v. ChoicePoint, Inc., No. 1:06-CV-0198-GET (N.D. Ga. Jan. 30, 2006) [hereinafter ChoicePoint Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf, *archived at* http://perma.cc/43MH-F7Y4; Complaint at 8, United States v. Rental Research Servs., Inc., No. 072-3228 (D. Minn. Mar. 5, 2009) [hereinafter Rental Research Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrscmpt.pdf, *archived at* http://perma.cc/UU8Y-VRSK;

failure in general to restrict access to those individuals with a valid need for the protected information.[174]

[64] System access control failures were a prominent feature of the $4.8 million settlements obtained by HHS in enforcement proceedings against New York and Presbyterian Hospital and Columbia University. The HHS investigation determined that the hospital and the university failed to assess and monitor the connection of computer applications and systems linked to the hospital's patient databases and failed to implement appropriate security measures and access procedures.[175]

[65] ISO 27002 offers a wealth of guidance on controls for system access, including controls regarding business requirements of access control, user access management, user responsibilities, and system and application access.[176]

---

[174] *See, e.g.*, Accretive Health Complaint at 2 ("[f]ailing to adequately restrict access to, or copying of, personal information based on an employee's need for information" and "[f]ailing to ensure that employees removed information from their computers for which they no longer had a business need"); *see also* LifeLock Complaint at 10 (failure "to limit access to personal information stored on or in transit through its networks only to employees and vendors needing access to the information to perform their jobs"); GeneLink and foru™ Complaint at 13 (creating unnecessary security risks by allowing service provider access to customers' complete personal information, rather than limiting access to only those categories of customer information for which service provider had a business need).

[175] *See* Press Release, U.S. Dep't of Health & Human Servs., Data Breach Results in $4.8 Million HIPAA Settlements (May 7, 2014) *available at* http://www.hhs.gov/news/press/2014pres/05/20140507b.html, *archived at* http://perma.cc/2QGN-9JCG.

[176] *See* ISO 27002, *supra* note 5, at § 9.1 (access control policy and network access); *see also id.* at § 9.2 (user registration, user access provisioning, management of privileged access rights, management of secret authentication information of users (e.g., passwords), review of user access rights, and removal or adjustment of access rights); *id.* at § 9.3 (use of secret authentication information (e.g., passwords); *id.* at § 9.4 (information access restriction, secure log-on procedures, password management systems, user of privileged utility programs, and access control to program source code).

[66] Through access control under the NIST Cybersecurity Framework's Protect function, "[a]ccess to assets…is limited to authorized users, processes, or devices, and to authorized activities and transactions." [177] Access control safeguards include "[i]dentities and credentials are managed for authorized devices and users; . . .[r]emote access is managed; . . . [a]ccess permissions are managed, incorporating the principles of least privilege and separation of duties; [and] . . . [n]etwork integrity is protected, incorporating network segregation where appropriate. "[178]

b. Physical Access Controls

[67] Physical access controls restrict access to physical locations, including computer facilities, workstations, and devices containing protected information, and are designed to permit access only to authorized individuals. [179] Such physical controls are commonly referenced in information security legal requirements.[180]

[177] Cybersecurity Framework, *supra* note 134, at 23.

[178] *Id.* at 23–24, 29 ("Access to systems and assets is controlled, incorporating the principle of least functionality").

[179] *See* FTC Business Guidance, *supra* note 63, at 8–9 (Physical Security under the "Lock It" Principle).

[180] *See, e.g.*, 12 C.F.R. Pt.30, app. B(III)(C)(1)(b) (2014) (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); *see also* 16 C.F.R. § 314.4(a) (2014) (FTC Safeguards Rule under Gramm-Leach-Bliley); 45 C.F.R. § 164.308(a)(4)(i) (2013) (The HIPAA Security Rule requires "policies and procedures for authorizing access to electronic protected health information . . . ."); 45 C.F.R. § 164.310(a)(1) (2013) ("policies and procedures to limit physical access to . . . electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed"); 45 C.F.R. § 164.310(b) (2013) ("policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information,"); 45 C.F.R. § 164.310(c) (2013) ("physical safeguards for all workstations

[68] On occasion, FTC enforcement actions have involved alleged lapses in physical facility safeguards, such as failure "to secure paper documents containing personal information that were received by facsimile in an open and easily accessible area."[181]

[69] ISO 27002 provides guidance on controls for facility and other physical access, including controls for physical security perimeters, physical entry controls, securing offices, rooms, and facilities, working in secure areas, and delivery and loading areas.[182] ISO 27002 also provides controls for equipment security.[183]

[70] The NIST Cybersecurity Framework addresses facility access in several subcategories of control activities, including "[p]hysical access to assets is managed and protected;" [184] and "[p]olicy and regulations regarding the physical operating environment for organizational assets are met."[185]

---

that access electronic protected health information, to restrict access to authorized users."); 45 C.F.R. § 164.310(a)(2) (2013) (Addressable implementation specifications include procedures for contingency operations, access of facility security plan, access control and validation procedures, and maintenance records related to physical security); *see also* 201 MASS CODE REGS.17.03(2)(e), (2)(g) (requiring "[r]easonable restrictions upon physical access to records containing personal information" and prevention of terminated employees from accessing records containing PII) (Massachusetts PII Protection Standards); OR. REV. STAT. ANN. § 646A.622(2)(d)(C)(iii)(West 2011) (safeguards to protect against unauthorized access to personal information) (Oregon PII Safeguards Statute).

[181] LifeLock Complaint at10.

[182] *See* ISO 27002, *supra* note 5, at § 11.1.

[183] *See id.* at § 11.2 (equipment siting and protection, cabling security, equipment maintenance, removal of assets, unattended user equipment, and clear desk and clear screen policies).

[184] Cybersecurity Framework, *supra* note 134, at 23.

c. Encryption

[71] Encryption of protected information is designed to control unauthorized access, either while the information is stored within the organization's systems or in storage devices and media ("data at rest"), or while the information being transmitted over and between networks, including the Internet ("data in transit").

[72] Encryption controls are referenced in some affirmative legal requirements for information security programs.[186] Effective encryption is generally also a safe harbor under laws requiring notification for breaches in the security of protected information.[187]

[73] The FTC has pursued companies in at least five enforcement matters for failure to encrypt protected information, most commonly credit card data, while in transmission.[188] In at least sixteen enforcement matters

---

[185] *Id.* at 27.

[186] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(1)(c) (2014) (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); *see also* 45 C.F.R. § 164.312(a)(2)(iv)(e)(2)(ii) (2013) (Under the HIPAA Security Rule, encryption is an addressable implementation specification regarding access control and for transmission security.). In addition, the Massachusetts PII Protection Standards require:

> To the extent technically feasible, . . . [e]ncryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly . . . [and] of all personal information stored on laptops or other portable devices.

201 MASS. CODE REGS. 17.04(3), (5) (Massachusetts PII Protection Standards).

[187] *See supra* text accompanying note 92.

[188] *See, e.g.*, BJ's Wholesale Club Complaint at 2 (failure to encrypt purchase card data in transit); *see also* LifeLock Complaint at 9 (transmitting protected information over its corporate network and the Internet in clear readable text); Compete Complaint at 5

the FTC has pursued companies under Section 5 of the FTC Act for storing protected information; most commonly card holder data, in clear readable text.[189] Most of these Section 5 enforcement actions for failure to encrypt data-at-rest were deception claims based on representations allegedly made by the company that protected information stored on the company's systems would be encrypted or otherwise secure.[190] However, in at least one enforcement matter the FTC has taken the position that storage of cardholder data in clear text, along with transmission of such cardholder data in clear text between in-store and corporate networks, is an unfair trade practice, without alleging any deceptive representation.[191]

(transmitting sensitive information, such as financial account numbers and security codes, from secure web pages in clear readable text over the Internet); TJX Complaint at 2 (transmitting protected information between in-store and corporate networks in clear text); Upromise Complaint at 4 (transmitting purchase card information in clear readable text over the Internet).

[189] *See, e.g.*, BJ's Wholesale Club Complaint at 2; *see also* ValueClick Complaint at 11; Wyndham Worldwide Complaint at 10; LifeLock Complaint at 9; Cbr Systems Complaint at 3; Ceridian Corp. Complaint at 2; DSW Complaint at 2; Genica Complaint at 2; Guess Complaint at 3; Guidance Software Complaint at 2; Life is Good Complaint at 2; Lookout Services Complaint at 3; Petco Complaint at 2–3; Complaint at 6, United States v. RockYou, Inc., No. 312-CV-01487-12 (F.T.C. Mar. 26, 2012) [hereinafter RockYou Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf, *archived at* http://perma.cc/52VR-52ZJ; TJX Complaint at 2; Twitter Complaint at 4.

[190] *See, e.g.*, Guidance Software Complaint at 2 ("we also do everything in our power to protect user-information off-line . . . ."); *see also* LifeLock Complaint at 9 ("All stored personal data is electronically encrypted."); ValueClick Complaint at 10 ("ValueClick also encrypts sensitive information such as passwords and financial data."); Life is Good Complaint at 2 ("All information is kept in a secure file . . . ."); Petco Complaint at 2 ("protecting your information is our number one priority, and your personal data is strictly shielded from unauthorized access. Our '100% Safeguard Your Shopping Experience Guarantee' means you never have to worry about the safety of your credit card information.").

[191] *See, e.g.*, TJX Complaint at 2–3.

[74] ISO 27002 provides guidance on cryptographic controls, including development and implementation of a policy on the use of such controls for information protection, and key management controls.[192]

[75] The NIST Cybersecurity Framework addresses Data Security under its Protect function, providing that "[d]ata-at-rest is protected," "[d]ata-in-transit is protected," and "[p]rotections against data leaks are implemented."[193]

d. Transmission Security Controls

[76] Various controls can be applied to help safeguard protected information in transmission over unsecured electronic communications networks, including the Internet. Such controls are designed to protect the integrity of the transmitted information and to guard against unauthorized access, such as through encryption.

[77] Some legal requirements for information safeguards explicitly address transmission security.[194] The FTC has taken the position in various enforcement proceedings that the transmission of protected information, such as cardholder data, in clear readable text is an unfair and deceptive trade practice.[195] ISO 27002 offers communication security

[192] *See* ISO 27002, *supra* note 5, at § 10.1.

[193] *See* Cybersecurity Framework, *supra* note 134, at 25–26.

[194] For example, the HIPAA Security Rule requires "technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." 45 C.F.R. § 164.312(e)(1) (2013); *see also* 45 C.F.R. § 164.312(e)(2)(i)–(ii) (2013) (outlining addressable implementation specifications of integrity controls and encryption).

[195] *See, e.g.*, BJ's Wholesale Club Complaint at 2; *see also* ValueClick Complaint at 11; Wyndham Worldwide Complaint at 10; LifeLock Complaint at 9; Cbr Systems Complaint at 3; Ceridian Corp. Complaint at 2; DSW Complaint at 2; Genica Complaint at 2; Guess Complaint at 3; Guidance Software Complaint at 2; Life is Good Complaint

controls regarding network security management and information transfers.[196] The NIST Cybersecurity Framework also addresses transmission security with several subcategories of control activities, including "[d]ata-in-transit is protected;" "[p]rotections against data leaks are implemented;" and "[c]ommunications and control networks are protected."[197]

e. Mobile Device & Portable Media Controls

[78] Various safeguard controls can be applied to address security risks inherent to protected information stored in mobile devices, such as laptops and smartphones, and in portable storage media.[198] Such controls may include inventorying and tracking of mobile devices and media, policies for proper use, access barriers to and encryption of mobile devices and media, and appropriate care in mobile device or media disposal and re-use.

[79] Some legal requirements for information safeguards directly address controls for mobile devices and portable media.[199] Mobile device

at 2; Lookout Services Complaint at 3; Petco Complaint at 2–3; RockYou Complaint at 6; TJX Complaint at 2; Twitter Complaint at 4.

[196] *See* ISO 27002, *supra* note 5, at § 13.1 (network controls, security of network services, and segregation in networks); *see also id.* at § 13.2 (information transfer policies and procedures, agreements on information transfer, and electronic messaging).

[197] Cybersecurity Framework, *supra* note 134, at 25–26, 29.

[198] *See* FTC Business Guidance, *supra* note 63 at 13–14.

[199] For example, the HIPAA Security Rule requires "policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility," 45 C.F.R. § 164.310(d)(1) (2013), "policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored," 45 C.F.R. § 164.310(d)(2)(i) (2013), and "procedures for removal of electronic protected health information from electronic media before the media are made available for re-use," 45 C.F.R. § 164.310(d)(2)(ii) (2013).

and portable media security has also been addressed in FTC enforcement actions under Section 5 of the FTC Act. In *Accretive Health*, a laptop stolen from an employee's locked car contained over 600 files with sensitive personal and health information of 23,000 patients, including patient names, dates of birth, billing information, diagnostic information, and Social Security numbers.[200] The FTC alleged that "[t]ransporting laptops containing personal information in a manner that made them vulnerable to theft or other misappropriation" constituted an unfair trade practice.[201] In *Cbr Systems, Inc.*, an employee's backpack was stolen from a personal vehicle; the backpack containing four Cbr backup tapes, a Cbr laptop, and a Cbr external hard drive and USB drive.[202] The unencrypted backup tapes contained protected personal and health information, and the unencrypted laptop and hard drive contained passwords and protocols for obtaining access to Cbr's network.[203] Similar to its position in *Accretive Health*, the FTC alleged that Cbr violated Section 5 by "transporting portable media containing protected information in a manner that made media vulnerable to theft or other misappropriation."[204] The FTC further pursued Cbr for "failing to take reasonable steps to render backup tapes or other portable media containing personal information or information that could be used to access personal information unusable, unreadable, or indecipherable in the event of unauthorized access . . . ."[205]

Addressable implementation specifications include maintaining a record of the movement of such hardware and media, and of the person responsible for it, and also data backup and storage. *See, e.g.*, 45 C.F.R. § 164.310(d)(2)(iii)(iv) (2013). For laws requiring reasonable controls for disposal of protected information and media and devices containing it, *see infra* text accompanying notes 254–264.

[200] *See* Accretive Health Complaint at 2.

[201] *See id.*

[202] *See* Cbr Systems Complaint at 3.

[203] *See id.*

[204] *Id.* at 2–3.

[80] In several recent enforcement matters, HHS has reached settlement agreements with HIPAA covered entities for failures to adequately secure ePHI in mobile devices and portable media. Adult & Pediatric Dermatology agreed to pay $150,000 for the disclosure of the ePHI of 2,200 individuals due to inadequate safeguards for a stolen, unencrypted thumb drive.[206] QCA Health Plan, Inc., reached a $250,000 resolution agreement to resolve an investigation of its failure to implement physical safeguards for an unencrypted laptop that contained ePHI of 148 individuals, and which was stolen out of a workforce member's car.[207] HHS has also obtained a $1.725 million settlement with Concentra Health Services, arising out of the theft of an unencrypted laptop from a Concentra facility, due to its failure to adequately inventory and assess encryption for its laptops, and its failure to implement sufficient policies and procedures for laptop security.[208]

[81] Under ISO 27002, organizations should adopt a "policy and supporting security measures . . . to manage the risks introduced by using mobile devices," and also a "policy and supporting security measures . . . to protect information accessed, processed or stored at teleworking sites."[209] Guidance is also offered for management of assets,[210] handling of assets,[211] media handling,[212] and management of equipment.[213]

---

[205] *Id* at 3.

[206] *See* Press Release, U.S. Dep't of Health & Human Servs., Dermatology Practice Settles Potential HIPAA Violations (Dec. 26, 2013), *available at* http://www.hhs.gov/news/press/2013pres/12/20131226a.html, *archived at* http://perma.cc/8929-2G99.

[207] *See* Press Release, U.S. Dep't of Health & Human Servs., Stolen Laptops Lead to Important HIPAA Settlements (Apr. 22, 2014), *available at* http://www.hhs.gov/news/press/2014pres/04/20140422b.html, *archived at* http://perma.cc/CM29-85YJ.

[208] *See id.*

[209] ISO 27002, *supra* note 5, at § 6.2.

[82] Under the NIST Cybersecurity Framework, control activities for mobile device and portable media security include "[a]ssets are formally managed throughout removal, transfers, and disposition," and "[r]emovable media is protected and its use restricted according to policy."[214]

f. System Change Management Controls

[83] At most organizations, computer applications and systems are in a nearly constant state of flux. System change management controls are designed to help ensure that security safeguards are not compromised in the acquisition, development, change, or retirement of computer systems.

[84] Some legal requirements for information safeguards explicitly require controls to ensure that changes to computer systems involving protected information do not exacerbate security risks.[215] Change management failures have also featured prominently in some FTC enforcement matters. For example, in *Credit Karma*, a security feature (SSL certificate validation) was disabled in the testing environment during

[210] *See id.* at § 8.1 (inventory of assets, ownership of assets, acceptable use of assets, and return of assets).

[211] *See id.* at § 8.2.3.

[212] *See id.* at § 8.3 (management of removable media, disposal of media, and physical media transfer).

[213] *See id.* at § 11.2.5 (removal of assets); *see also id.* at § 11.2.6 (security of equipment and assets off-premises); *id.* at § 11.2.7 (secure disposal or re-use of equipment).

[214] Cybersecurity Framework, *supra* note 134, at 25, 29.

[215] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(1)(d) (2014) ("[p]rocedures designed to ensure that customer information system modifications are consistent with the bank's information security program") (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley).

development of a smartphone application, but the security feature was not re-enabled before the application was launched to consumers.[216] In *HTC America*, website developers activated code during application development to capture and log information, but failed to deactivate the code before the smartphones and tablet devices were shipped to customers.[217] In *MTS, Inc.*, the respondent companies redesigned the "check out" portion of their website, rewriting software code for the Order Status application, but failed to ensure that certain code from the original version had been included in the new version, resulting in protected information being accessible in clear text.[218] The FTC alleged that respondents failed to "implement appropriate checks and controls on the process of writing and revising Web applications . . . ."[219]

[85] System change management controls have also been the focus of HIPAA enforcement. In 2013, management care company WellPoint Inc. agreed to pay the U.S. Department of Health and Human Services $1.7 million to resolve an investigation which determined that WellPoint failed to perform an appropriate technical evaluation of a software upgrade in its online application database, resulting in the ePHI of over 612,000 individuals being accessible over the Internet.[220]

[86] ISO 27002 offers guidance on a variety of controls covering both management of information system changes to ensure continued effectiveness of safeguards, and also prohibiting unauthorized changes in

[216] *See* Credit Karma Complaint at 3; *see also* Fandango Complaint at 3–4 (failure to restore Apple security default settings before releasing mobile application to customers).

[217] *See* HTC America Complaint at 5.

[218] *See* MTS and Tower Direct Complaint at 3.

[219] *See id.* at 4.

[220] *See* Press Release, U.S. Dep't of Health & Human Servs., WellPoint Pays HHS $1.7 Million for Leaving Information Accessible Over Internet (July 11, 2013) *available at* http://www.hhs.gov/news/press/2013pres/07/20130711b.html, *archived at* http://perma.cc/CFM2-A5B4.

information systems.[221] ISO 27002 also includes a range of controls for information system changes occurring through system acquisition, development, and maintenance activities, including the inclusion of information security in identifying requirements for new information systems or enhancements to existing information systems, [222] in development and support processes for information systems,[223] and for the protection of test data.[224]

[87] The NIST Cybersecurity Framework provides a variety of control activities related to system change management under the Information Protection Processes and Procedures category, including "[a] baseline configuration of information technology/industrial control systems is created and maintained;" "[a] System Development Life Cycle to manage systems is implemented;" "[c]onfiguration change control processes are in place;" and "[a] vulnerability management plan is developed and implemented."[225] Additional control activities include "[t]he development and testing environment(s) are separate from the production environment," and control activities for approved maintenance and repair or organizational assets, including remote maintenance.[226]

[221] *See* ISO 27002, *supra* note 5, at §§ 12.1.2-12.1.4, 12.5.1, 12.6.

[222] *See id.* at § 14.1.1.

[223] *See id.* at § 14.2.

[224] *See id.* at § 14.3.1.

[225] Cybersecurity Framework, *supra* note 134, at 26–28.

[226] *See id.* at 27–28.

g. Employee Management Controls

[88] Various safeguards controls are designed to address security risks involving the organization's employees. Beyond training (discussed below), controls may address employee selection and authorization to access protected information, segregation of duties involving protected information, discipline for security infractions, and controls regarding separated employees. Various legal requirements for information safeguards address employee security controls.[227]

[89] ISO 27002 provides controls for information security in human resource activities, including activities prior to employment,[228] during

[227] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(1)(e) (2014) ("[d]ual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information") (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); 16 C.F.R. §§ 314.4(b)(1), (c) (2014) (requiring information safeguards to control identified risks, including risks involving "[e]mployee training and management") (FTC Safeguards Rule under Gramm-Leach-Bliley); *see also* 201 MASS. CODE REGS. 17.03(2)(d), (e) (2014) (requiring "disciplinary measures for violations of the comprehensive information security program rules" and prevention of terminated employees from accessing records containing PII) (Massachusetts PII Protection Standards); OR. REV. STAT. ANN. § 646A.622(2)(d)(A)(iv) (West 2011) (information security program deemed compliant if, among other matters, it includes managing of employees on security program practices and procedures) (Oregon PII Safeguards Statute).

The HIPAA's Security Rule requires application of "appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate," 45 C.F.R. § 164.308(a)(1)(ii)(C) (2013).

HIPPA's Security Rule also requires "policies and procedures to ensure that all members of [the] workforce have appropriate access to electronic protected health information . . . and to prevent those workforce members who do not have access . . . from obtaining access to electronic protected health information." 45 C.F.R. § 164.308(a)(3)(i) (2013). Addressable implementation specifications include employee authorization and supervision, procedures for workforce clearance to access ePHI, and procedures for termination of such access upon employee separation. 45 C.F.R. § 164.308(a)(3)(ii) (2013).

employment, [229] and on termination or change of employment. [230] Guidance is also offered for controls regarding employee confidentiality or nondisclosure agreements. [231] Under the NIST Cybersecurity Framework, "[c]ybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)."[232]

h. Environmental Risk Controls

[90] Protected information can be at risk for loss or damage due to environmental hazards, such as fire or water damage, or failures in computer systems. Controls for environmental hazards are designed to help ensure the integrity and safeguarding of information throughout the course of such events. Some laws requiring information safeguards specifically mandate controls for environmental hazards.[233]

[91] Under ISO 27002, "[p]hysical protection against natural disasters, malicious attack or accidents should be designed and applied." [234]

---

[228] *See* ISO 27002, *supra* note 5, at § 7.1.

[229] *See id.* at § 7.2

[230] *See id.* at § 7.3.1.

[231] *See id.* at § 13.2.4.

[232] Cybersecurity Framework, *supra* note 134, at 28.

[233] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(1)(h) (2014) (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley). The HIPAA Security Rule requires "policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information," including data backup plans, disaster recovery plans, and emergency mode operation plans. *See* 45 C.F.R. §§ 164.308(a)(7)(i), (ii)(A)–(C) (2013). Addressable implementation specifications include testing and revision procedures and analysis of applications and data criticality. *See, e.g.*, 45 C.F.R. § 164.308(a)(7)(ii)(D)–(E) (2013).

[234] *See* ISO 27002, *supra* note 5, at § 11.1.4.

Guidance is offered on controls for environmental risks involving equipment.[235] "Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy."[236] Control guidance is also provided on information security continuity[237] and availability of redundant information processing facilities.[238] Control activities for environmental hazards under the NIST Cybersecurity Framework include "[d]ata-at-rest is protected" and "[b]ackups of information are conducted, maintained, and tested periodically."[239]

i. Monitoring & Detection Controls

[92] This family of safeguard controls is designed to help the organization be cognizant of activity involving protected information, including monitoring for unauthorized intrusion or access and protection against and detection of malware or system attacks.[240] Such controls may involve logging and audit controls, system activity reviews, and use of software for prevention and detection. Legal requirements for information safeguards commonly address system monitoring and detection controls.[241]

---

[235] *See e.g.*, *id.* at § 11.2 (for example, equipment siting and protection, supporting utilities, and cabling security).

[236] *Id.* at § 12.3.1.

[237] *See, e.g.*, *id.* at § 17.1 (planning information security continuity; implementing information security continuity; verify, review and evaluate information security continuity).

[238] *See, e.g.*, *id.* at § 17.2.1.

[239] Cybersecurity Framework, *supra* note 134, at 25, 27.

[240] *See, e.g.*, FTC Business Guidance, *supra* note 63 at 17 ("Detecting Breaches" under the "Lock It" Principle).

[241] *See, e.g.*, 12 C.F.R. pt. 30, app. B (III)(C)(1)(f) (2014) ("[m]onitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer

[93] The FTC has frequently alleged in its data security enforcement actions that the respondent company failed to employ sufficient measures to monitor and detect unauthorized access to consumers' personal information,[242] such as in *Cbr Systems, Inc.*, where FTC alleged that the respondent

information systems") (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); 16 C.F.R. §§ 314.4(b)(3), (c) (2014) (requiring information safeguards to control identified risks, including risks in "[d]etecting, preventing and responding to attacks, intrusions, or other systems failures.") (FTC Safeguards Rule under Gramm-Leach-Bliley).

The HIPAA Security Rule requires "procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports," 45 C.F.R. § 164.308(a)(1)(ii)(D) (2013), implementation of "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information," 45 C.F.R. § 164.312(b) (2013), and "policies and procedures to protect electronic protected health information from improper alteration or destruction," 45 C.F.R. § 164.312(c)(1) (2013).

Addressable implementation specifications include "procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports," 45 C.F.R. § 164.308(a)(1)(ii)(D) (2013), "[p]rocedures for guarding against, detecting, and reporting malicious software," 45 C.F.R. § 164.308(a)(5)(ii)(B) (2013), "[p]rocedures for monitoring log-in attempts and reporting discrepancies," 45 C.F.R. § 164.308(a)(5)(ii)(C) (2013), and implementing "electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an authorized manner," 45 C.F.R. § 164.312(c)(2) (2013).

The Massachusetts PII Protection Standards require, "to the extent technically feasible . . . [r]easonable monitoring of systems, for unauthorized use of or access to personal information, . . . [r]easonably up-to-date firewall protection and operating system security patches" for files containing PII on systems connected to the Internet; and "reasonably up-to-date versions of system security agent software . . . ." *See* 201 MASS. CODE REGS. 17.04(4), (6), (7) (2014); *see also* OR. REV. STAT. ANN. §§ 646A.622(2)(d)(B)(iii), (C)(ii) (West 2011) (information security program deemed compliant if it includes, among other matters, detection and prevention for attacks or system failures and detection and prevention for intrusions) (Oregon PII Safeguards Statute).

> Failed to employ sufficient measures to prevent, detect, and investigate unauthorized access to computer networks, such as by adequately monitoring web traffic, confirming distribution of anti-virus software, employing an automated intrusion detection system, retaining certain system logs, or systematically reviewing system logs for security threats.[243]

[94] ISO 27002 offers controls regarding system logging and monitoring,[244] information systems audit controls,[245] and detecting, preventing, and recovering from malware.[246]

[95] Logging and monitoring activities are addressed in the NIST Cybersecurity Framework, including "[i]ntegrity checking mechanisms are used to verify software, firmware, and information integrity," and [a]udit/log records are determined, documented, implemented, and reviewed in accordance with policy."[247] Under the Security Continuous Monitoring category,

> The network is monitored to detect potential cybersecurity events; . . . [t]he physical environment is monitored to detect potential cybersecurity events; . . .[p]ersonnel

[242] *See, e.g.*, LifeLock Complaint at 9–10; BJ's Wholesale Club Complaint at 2; Cardsystems Solutions Complaint at 2; Cbr Systems Complaint at 2–3; ChoicePoint Complaint at 9; DSW Complaint at 2; Genica Complaint at 2–3; Guidance Software Complaint at 2; LabMD Complaint at 3; Microsoft Complaint at 2.

[243] Cbr Systems Complaint at 3.

[244] *See* ISO 27002, *supra* note 5, at § 12.4 (setting standards for event logging, protection of log information, administrator and operator logs, and clock synchronisation).

[245] *See id*. at § 12.7.1.

[246] *See id*. at § 12.2.1.

[247] *See* Cybersecurity Framework, *supra* note 134, at 26, 29.

> activity is monitored to detect potential cybersecurity events; . . . [m]alicious code is detected; . . . [u]nauthorized mobile code is detected; . . . [e]xternal service provider activity is monitored to detect potential cybersecurity events; . . . [m]onitoring for unauthorized personnel, connections, devices, and software is performed; [and] . . . [v]ulnerability scans are performed.[248]

Also, under the Detection Processes category, "[r]oles and responsibilities for detection are well defined to ensure accountability; . . . [d]etection activities comply with all applicable requirements; . . . [d]etection processes are tested; . . . [e]vent detection information is communicated to appropriate parties; [and] . . . [d]etection processes are continuously improved."[249]

j. Retention Controls

[96] An additional safeguard measure for protected information is to ensure that it is not retained for longer than is necessary to comply with legal retention requirements and business need.[250] It is not possible to have a security breach compromising protected information that no longer exists, having been compliantly disposed of once its legally required retention and business value have expired.

[97] Some legal requirements for information security programs explicitly address disposal of protected information once it has served its valid business purpose. For example, contracts between HIPAA covered entities and business associates must require that the business associate "[a]t termination of the contract, if feasible, return or destroy all protected

[248] *See id*. at 30–31.

[249] *Id*. at 31–32.

[250] *See, e.g.*, FTC Business Guidance, *supra* note 63, at 6–7 (referencing the "Scale Down" Principle and "keep[ing] only what you need for your business").

health information received from, or created or received by the business associate on behalf of, the covered entity."[251]

[98] In several data security enforcement matters the FTC has found fault with companies' unnecessary retention of protected information, alleging that such practices create unnecessary risks to the information's security.[252]

[99] The NIST Cybersecurity Framework includes as a control activity that "[d]ata is destroyed according to policy."[253] It is presumably fair to interpret this control as pertaining not only to policies for compliant means of disposal, but also to policies regarding the length of time categories of information are kept by the organization, such as retention schedules.

k. Disposal Controls

[100] Various safeguards may be employed to control risks in connection with the ultimate disposal of protected information. Such controls should also address the disposal, return, and re-use of hardware devices and media that contain protected information,[254] as well as the destruction of protected information in hard copy media.

[251] 45 C.F.R. § 164.504(e)(2)(J) (2013). The HIPAA Privacy Rule "return or destroy" requirement applies to all such PHI and all copies, and if return or destruction is not feasible, the contract must extend safeguard obligations to such information remaining in the business associate's custody. *Id.*

[252] *See, e.g.*, BJ's Wholesale Club Complaint at 2; Cbr Systems Complaint at 3; Ceridian Corp. Complaint at 2; DSW Complaint at 2; Life is Good Complaint at 2.

[253] Cybersecurity Framework, *supra* note 134, at 27.

[254] *See* Press Release, U.S. Dep't of Health & Human Servs., HHS Settles with Health Plan in Photocopier Breach Case (Aug. 14, 2013) *available at* http://www.hhs.gov/news/press/2013pres/08/20130814a.html (explaining that in 2013, Affinity Health Plan Inc. agreed to pay over $1.2 million to resolve an HHS investigation under HIPAA, which determined that Affinity Health returned multiple copiers to its leasing company without erasing data on the copiers' hard drives, exposing ePHI of

[101] A wide range of information security requirements address proper disposal of storage devices or media containing such information. Legal requirements for information security programs commonly include controls for disposal of protected information.[255] As noted previously, the FACTA Disposal Rules of various regulators require that reasonable measures be taken in disposing of protected customer information to safeguard against "unauthorized access to or use of the information in connection with its disposal."[256] A majority of states require entities with PII of state residents to have disposal safeguards, mandating either a disposal policy for PII[257] or compliant practices for reasonable disposal of PII—such as the shredding of hardcopy documents, affective erasure of electronic media, or other actions to render PII unreadable or indecipherable.[258] Many organizations contract with service providers for disposal of documents and electronic data containing protected information. Legal requirements for disposal contracting are discussed below.[259]

almost 345,000 individuals), *archived at* http://perma.cc/L7YB-3GCV; *see also* FTC. Business Guidance, *supra* note 63, at 15 (referencing the digital copiers under the "Lock It" principle); *id.* at 21 (citing the "Pitch It" principle that one should "properly dispose of what you no longer need.").

[255] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(4) (2014) (citing the interagency guidelines establishing information security standards under Gramm-Leach-Bliley); 16 C.F.R. § 314.4(b)–(c) (2014) (requiring information safeguards to control identified risks, including risks in information disposal); 45 C.F.R. § 164.310(d)(2)(i) (2013) (requiring "policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.").

[256] *See supra* note 26.

[257] *See supra* note 33 and accompanying text.

[258] *See supra* note 34 and accompanying text.

[259] *See infra* text accompanying notes 287–88.

[102] The FTC has entered into consent orders with several companies for failing to comply with disposal safeguards under FACTA and Gramm-Leach-Bliley.[260] In enforcement actions against national pharmacy chains, the FTC has alleged that widespread unsecure disposal of customer personal information is an unfair and deceptive trade practice.[261]

[103] ISO 27002 offers controls related to disposal of media containing protected information[262] and for secure disposal or re-use of equipment containing protected information.[263]

---

[260] *See, e.g.*, American United Complaint at 3–4 (Under FACTA Disposal Rule, failure to implement reasonable procedures for disposal of customers' personal information, customer personal information repeatedly found in unsecured dumpster and open trash bags); Complaint at 5–6, FTC v. Gregory Navone, No. 2:08-cv-01842(D. Nev. Dec. 30, 2008) [hereinafter Navone Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf (Under FACTA, failure to oversee collection and transport of personal information for disposal, 40 boxes containing tax returns, mortgage applications, bank statements, copies of credit cards and drivers' licenses, and consumer reports found in publically accessible dumpster), *archived at* http://perma.cc/X2XB-C5YB; Complaint at 5–6, United States v. PLS Financial Services, Inc., No. 1:12-cv-08334 (N.D. Ill. Oct. 17, 2012) [hereinafter PLS Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121107plspaydaycmpt.pdf (Under FACTA, failure to take reasonable measures against unauthorized access or use of consumer report information in disposal, documents containing customer names, Social Security numbers, wage and bank account information, cancelled checks, loan applications and agreements, and consumer reports found in unsecured, easily accessible dumpsters), *archived at* http://perma.cc/H7C7-GM97; Nations Title Agency Complaint at 1-2 (Under Gramm-Leach-Bliley, failure to implement reasonable procedures for disposal of personal information, television station found intact documents with sensitive personal information discarded in unsecured dumpster).

[261] *See, e.g.*, CVS Complaint at 2–3 (failure to implement procedures to securely dispose of customers' personal information, discarding materials containing personal information in clear readable text in unsecured, public trash dumpsters, media outlets reported finding such personal information in unsecured dumpsters in at least fifteen cities); Rite Aid Complaint at 2–3 (failure to implement secure disposal procedures, discarding materials containing personal information in clear readable text in unsecured dumpsters, media reports of finding personal information in unsecured dumpsters in at least seven cities).

[262] *See* ISO 27002, *supra* note 5, at § 8.3.2.

[104] The NIST Cybersecurity Framework includes subcategories of control activities for secure disposal, including "[a]ssets are formally managed throughout removal, transfers, and disposition" and "[d]ata is destroyed according to policy."[264]

3. Training

[105] An organization should use training and other awareness-building efforts to help ensure that its employees understand their responsibilities regarding information security.[265] Training is commonly referenced in legal requirements for information security programs.[266] Inadequate training is also frequently cited by the FTC in its enforcement proceedings, including employee guidance and training on such matters as

[263] *See id.* at § 11.2.7.

[264] Cybersecurity Framework, *supra* note 134, at 25, 27.

[265] *See* FTC Business Guidance, *supra* note 63, at 17 ("Employee Training" under the "Lock It" Principle).

[266] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(2) (2014) (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); 16 C.F.R. § 314.4(b)(1), (c) (2014) (implement safeguards to control identified risks, including "[e]mployee training and management") (FTC Safeguards Rule under Gramm-Leach-Bliley). The HIPAA Security Rule requires covered entities and business associates to "[i]mplement a security awareness and training program for all members of its workforce (including management)." 45 C.F.R. § 164.308(a)(5)(i) (2013). Addressable implementation specifications include periodic security updates and procedures for protecting against, detecting, and reporting malware. 45 C.F.R. § 164.308(a)(5)(ii)(A)–(B) (2013); *see also* 201 MASS. CODE REGS. 17.03(2)(b)(1), 17.04(8) (2014) (requiring risk assessment to evaluate and improve effectiveness of "ongoing employee (including temporary and contract employee) training" and also requiring "[e]ducation and training of employees on the proper use of the computer security system and the importance of personal information security.") (Massachusetts PII Protection Standards); OR. REV. STAT. ANN. § 646A.622(2)(d)(A)(iv) (West 2011) (information security program deemed compliant if it includes, among other matters, training of employees on the security program practices and procedures) (Oregon PII Safeguards Statute).

privacy and information security generally;[267] the prevention of unauthorized disclosure of personal information;[268] proper design, review, and testing of security for applications and software, for employees with those responsibilities;[269] secure access from remote locations;[270] proper response to security incidents;[271] and secure disposal.[272]

[106] Under ISO 27002, "[a]ll employees of the organization and, where relevant, contractors should receive appropriate [information security] awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function."[273]

[107] Awareness and Training under the NIST Cybersecurity Framework means that "[t]he organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements."[274] NIST training and awareness measures include "[a]ll users are informed and trained," and roles and responsibilities are understood by "privileged users," "third-party stakeholders (e.g., suppliers, customers, partners)," "[s]enior executives," and "[p]hysical and information security personnel."[275]

[267] *See, e.g.*, Eli Lily Complaint at 3; Nationwide Complaint at 3; Upromise Complaint at 4–5.

[268] *See, e.g.*, EPN Complaint at 2.

[269] *See, e.g.*, MTS and Tower Direct Complaint at 3–4; TRENDnet Complaint at 4–5.

[270] *See, e.g.*, Sunbelt Lending Complaint at 2.

[271] *See, e.g.*, Goal Financial Complaint at 2.

[272] *See, e.g.*, CVS Complaint at 2; PLS Complaint at 5–6; Rite Aid Complaint at 2–3.

[273] ISO 27002, *supra* note 5, at § 7.2.2.

[274] Cybersecurity Framework, *supra* note 134, at 24.

[275] *Id*. at 24–25.

4. Testing

[108] Organizations should have a reasonable approach to testing and monitoring the effectiveness of their information security policies, procedures, and controls to determine whether they are operating as intended. Such testing is generally more reliable if it is performed by an independent internal staff or independent third-parties, rather than by individuals responsible for the particular security function or control being tested.

[109] Testing and monitoring of security controls feature prominently in legal requirements for information security programs.[276] Under the U.S.-EU Safe Harbor Framework's Enforcement Principle "procedures for verifying that the commitments companies make to adhere to the safe

[276] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(3) (2014). The Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley state:

> Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

Id.; *see* also16 C.F.R. § 314.4(c) (2014)("[R]egularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.") (FTC Safeguards Rule under Gramm-Leach-Bliley); 45 C.F.R. § 164.308(a)(8) (2013) ("Perform a periodic technical and nontechnical evaluation . . . that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.") (HIPAA Security Rule); *see also* 201 MASS. CODE REGS. 17.03(2)(h) (2013) (requiring "[r]egular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information . . . .") (Massachusetts PII Protection Standards); OR. REV. STAT. ANN. § 646A.622(2)(d)(B)(iv) (West 2011) (requiring an information security program that "[r]egularly tests and monitors the effectiveness of key controls, systems, and procedures" to bring it into compliance with the statute) (Oregon PII Safeguards Statute).

harbor principles have been implemented . . . ,"[277] either through self-assessment or outside compliance reviews.[278] Additionally, FTC consent orders commonly require "regular testing and monitoring of the effectiveness of the safeguards' key controls, systems, and procedures."[279] Such consent orders generally also require periodic assessments and reports of the security program's effectiveness by "a qualified, objective, independent third-party professional who uses procedures and standards generally accepted in the profession."[280]

[110] Under ISO 27002, "[t]he organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur."[281] "Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements."[282] And, "[i]nformation systems should be regularly reviewed for compliance with the organization's information security

[277] *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last visited Oct. 1, 2014), *archived at* http://perma.cc/GKH9-ZLAX.

[278] *See U.S.-EU Safe Harbor FAQ 7-Verification*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018379.asp (last visited Oct. 1, 2014), *archived at* http://perma.cc/MUV4-8MBR.

[279] *See* Accretive Health Order at 3; *see also* consent orders cited supra note 43 (consent orders under Gramm-Leach-Bliley); consent orders cited supra note 45 (consent orders under COPPA); *and* consent orders cited supra notes 51, 52, and 54 (consent orders under FTC Act § 5).

[280] *E.g.*, Accretive Health Order at 3; *see also* consent orders cited supra notes 43, 45, 51, 52, and 54.

[281] ISO 27002, *supra* note 5, at § 18.2.1.

[282] *Id.* at § 18.2.2.

policies and standards."[283] Such technical compliance review can involve penetration tests or vulnerability assessments, and, if so, "caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable."[284] Additionally, the NIST Cybersecurity Framework includes activities for testing security controls, including "[v]ulnerability scans are performed" and "[d]etection processes are tested."[285]

D. Contract

An Organization Should Address the Security of Protected Information in its Third-Party Relationships

[111] In a reasonable information security program, an organization should address identified threats, vulnerabilities, and risks to the security of protected information arising from its relationships with third-parties that receive, create, maintain, or transmit protected information on the organization's behalf.[286] Consideration should also be given to third-parties that do not have custody of the organization's protected information, but that nevertheless have direct or indirect access to the organization's computer systems, thereby creating vulnerabilities for hacking or other intrusions.

[112] Legal requirements for information security commonly mandate that the safeguarding of protected information be addressed in third-party relationships. Various safeguard rules promulgated under Gramm-Leach-Bliley require oversight of service provider arrangements in three phases

[283] *Id.* at § 18.2.3.

[284] *Id.*

[285] Cybersecurity Framework, *supra* note 134, at 31–32.

[286] *See* FTC Business Guidance, *supra* note 63, at 19 (explaining the "Security Practices of Contractors and Service Providers" under the "Lock It" Principle).

of the relationship: due diligence in service provider selection; contracting that obligates the service provider to implement appropriate security measures; and monitoring of service provider performance in that regard.[287] The HIPAA Security Rules require compliant written business associate agreements between covered entities and business associates, and also between business associates and subcontractors, who "create, receive, maintain, or transmit electronic protected health information on the covered entity's [or business associate's] behalf."[288]

[113] Under California, Maryland, Nevada, and Rhode Island laws, businesses that disclose state residents' PII to non-affiliated third-parties must contract with them to require such third-parties to establish PII security procedures and practices.[289] Massachusetts and Oregon mandate information security programs that, among other matters, require PII protection to be addressed in service provider contracts.[290]

[114] Federal and state laws also address contracting with service providers for disposal of protected information. For example, the FTC's Disposal Rule under FACTA provides that organizations must comply with their obligation to properly dispose of consumer information by, "[a]fter due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction

[287] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(D)(1)–(3) (2014) (regarding monitoring, "a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers") (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); 16 C.F.R. § 314.4(d)(1) –(2) (2014) (detailing the FTC Safeguards Rule under Gramm-Leach-Bliley).

[288] *See* 45 C.F.R. § 164.308(b)(1) (2013); *see also* 45 C.F.R. § 164.314(a) (2013).

[289] *See, e.g.*, CAL. CIV. CODE § 1798.81.5(c) (LexisNexis Supp. 2014); MD. CODE ANN., COM. LAW § 14-3503(b)(1) (LexisNexis Supp. 2013); NEV. REV. STAT. § 603A.210(2) (LexisNexis Supp. 2010); R.I. GEN. LAWS § 11-49.2-2(3) (Supp. 2013).

[290] *See, e.g.*, 201 MASS. CODE REGS. 17.03(2)(f)(2) (2014); OR. REV. STAT. ANN. § 646A.622(2)(d)(A)(v) (West 2011).

to dispose of material, specifically identified as consumer information, in a manner consistent with this rule."[291] Various states, including Alaska, Hawaii, Illinois, North Carolina, and South Carolina, similarly require compliant contracting with service providers for PII disposal.[292]

[115] Under its Gramm-Leach-Bliley enforcement authority, the FTC has pursued companies for failure to ensure—by contract—that their service providers will protect the security and confidentiality of protected information.[293] The FTC has also taken the position that inadequate contracting and oversight for service providers with protected information access can constitute an unfair and deceptive trade practice under Section

[291] 16 C.F.R. § 682.3(b)(3) (2014). The Disposal Rule under FACTA provides examples of compliant due diligence, including:

> Reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.

Id.; *see also supra* note 26 (highlighting that Disposal Rules in regulations for other financial institutions).

[292] *See, e.g.*, ALASKA STAT. § 45.48.510(3) (2012); HAW. REV. STAT. ANN. § 487R-2(c) (LexisNexis Supp. 2012); 815 ILL. COMP. STAT. § 530/40(c) (West Supp. 2013); N.C. GEN. STAT. § 75-64(c) (2013); S.C. CODE ANN. § 37-20-190(B) (Supp. 2013).

[293] *See, e.g.*, Goal Financial Complaint at 2 (failing "to require third-party service providers by contract to protect the security and confidentiality of personal information."); James B. Nutter & Co. Complaint at 2 (providing "back-up tapes containing personal information in clear readable text to a third-party service provider," without requiring the service provider to protect the information's security and confidentiality); Nations Title Agency Complaint at 2 (failing to provide reasonable oversight for handling of personal information by service providers employed to process and assist in real estate closings); Sunbelt Lending Complaint at 2 (failing to take steps to ensure service providers were providing appropriate security for customer information).

5 of the FTC Act. For example, in *GeneLink, Inc. and foru*^{TM} *International Corporation*, the respondent companies collected customers' genetic information for the purpose of "tailoring" skincare products and nutritional supplements to the genetic circumstances of customers. GeneLink and foru^{TM} permitted their service providers to access collected personal information in order to maintain GeneLink and foru^{TM}'s customer relationship databases, fulfill customer orders, and develop related applications.[294] According to the FTC, GeneLink and foru^{TM} "[f]ailed to require by contract that service providers implement and maintain appropriate safeguards for consumers' personal information" and "[f]ailed to provide reasonable oversight of service providers, for instance by requiring that service providers implement simple, low-cost, and readily available defenses to protect consumers' personal information."[295] The resulting consent decrees required GeneLink and foru^{TM} to develop and use "reasonable steps to select and retain service providers capable of appropriately safeguarding Personal Information received" from the companies, and further required them to require "service providers by contract to implement and maintain appropriate safeguards . . . ."[296]

[116] FTC enforcement actions have also addressed service provider relationships in which protected information was not made accessible to the service provider, but that nevertheless created risks to the security of protected information. For example, in *Wyndham*, a pending enforcement lawsuit under Section 5 of the FTC Act, the FTC has alleged it is a deceptive and unfair trade practice to fail to restrict service provider network access, "such as by restricting connections to specified IP addresses or granting temporary, limited access, as necessary." [297]

[294] *See, e.g.*, GeneLink and foru^{TM} Complaint at 12.

[295] *Id.* at 13.

[296] *See* GeneLink Order at 7; Consent Order at 7, *In re* foru^{TM} Int'l. Corp., No. C-4457 (F.T.C. May 8, 2014) [hereinafter foru^{TM} Order], http://www.ftc.gov/system/files/documents/cases/140512foruintdo.pdf, *archived at* http://perma.cc/TP5Z-97RF.

Similarly, in the matter of *Credit Karma*, also an enforcement action under Section 5 of the FTC Act, the FTC alleged that it was a deceptive and unfair practice for the respondent to fail in providing "reasonable oversight of its service providers during the development process" of a mobile application that allegedly allowed unauthorized access to protected information.[298]

[117] FTC Consent Orders commonly require "[t]he development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards."[299]

[118] ISO 27002 offers guidance and controls for establishing information security in supplier relationships, including information security policies for supplier relationships, addressing security within supplier agreements, and establishing security requirements for the information and communication technology supply chain.[300] Controls are also provided for monitoring and review of supplier services and managing changes to supplier services.[301] Control guidance is also

[297] Wyndham Worldwide Complaint at 2, 12; *see also* LifeLock Complaint at 10 (alleging that the company "[f]ailed to require . . . vendors, and others with access to personal information to use hard-to-guess passwords or to implement related security measures, such as periodically changing passwords or suspending users after a certain number of unsuccessful log-in attempts . . . .").

[298] Credit Karma Complaint at 4.

[299] *See, e.g.*, Accretive Health Order at 3; *see also* consent orders cited *supra* note 45 (consent orders under Gramm-Leach-Bliley Act and COPPA containing similar language); *and* consent orders cited *supra* notes 51–52, 54 (consent orders under FTC Act § 5 containing similar language).

[300] ISO 27002, *supra* note 5, at §§ 15.1.1–15.1.3.

[301] *See id.* at §§ 15.2.1–15.2.2.

provided regarding agreements on information transfer and confidentiality and non-disclosure agreements.[302]

[119] The NIST Cybersecurity Framework provides control activities regarding third parties, including "[c]ybersecurity roles and responsibilities for . . . third-party stakeholders (e.g., suppliers, customers, partners) are established"; "[i]nformation security roles & responsibilities are coordinated and aligned with . . . external partners"; and "[t]hird-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities."[303]

E. Respond

An Organization Should Respond to Detected Breaches of the Security of Protected Information

[120] Organizations should be prepared to respond to detected breaches in the security of protected information, consistent with applicable legal requirements and obligations to third-parties.[304] Legal requirements for information security programs commonly require that covered organizations have the capability to respond when unauthorized access to protected information occurs.[305]

---

[302] *See id.* at §§ 13.2.2, 13.2.4.

[303] Cybersecurity Framework, *supra* note 134, at 20–21, 24.

[304] *See* FTC Business Guidance, *supra* note 63 at 22–23 (the "Plan Ahead" Principle, "[c]reate a plan for responding to security incidents.").

[305] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(C)(1)(g) (2014) (requiring "[r]esponse programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies . . . .") (Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley); 16 C.F.R. § 314.4(b)(3), (c) (2014) (requiring safeguards to control identified risks, including in detecting and responding "to attacks, intrusions, or other systems failures.") (FTC Safeguards Rule under Gramm-Leach-Bliley); HIPAA Security Rule, 45 C.F.R. §

[121] Numerous laws require breach notification to affected individuals and, in certain circumstances, to governmental and other authorities if a breach occurs to protected information. HIPAA breach notifications are governed by 45 C.F.R. Part 164, Subpart D. Though the Gramm-Leach-Bliley Act does not itself require breach notification, the rules of various entities that regulate financial institutions promulgated under Gramm-Leach-Bliley require such notifications be made as part of the institution's mandated response programs.[306] As discussed previously, forty-seven states, Puerto Rico, Guam, and the U.S. Virgin Islands require covered businesses with PII of the jurisdiction's residents to provide notice if an unauthorized disclosure or breach of PII occurs.[307]

[122] ISO 27002 provides a series of controls regarding information security incident management, addressing such matters as responsibilities and procedures, reporting information security events, reporting information security weaknesses, assessment of and decisions responding to information security events, learning from information security incidents, and collection of evidence.[308]

164.308(a)(6) (2013) (requiring "policies and procedures to address security incidents" and covered entities and business associates to "[i]dentify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes."); *see also* Massachusetts PII Protection Standards, 201 MASS. CODE REGS. 17.03(2)(j) (2014) (requiring "[d]ocumenting responsive actions taken in connection with any incident involving a breach of security . . . ."); Oregon PII Safeguards Statute, OR. REV. STAT. ANN. §§ 646A.622(2)(d)(B)(iii), (C)(ii) (West 2011) (information security program deemed compliant if it includes detection and response to attacks or system failures and intrusions).

[306] *See, e.g.*, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. pt. 30, app. B, supp. A (2014); Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice (NCUA), 12 C.F.R. pt. 748, app. B (2014).

[307] *See supra* text accompanying note 89.

[308] ISO 27002, *supra* note 5, at §§ 16.1.1-16.1.4, 16.1.6, 16.1.7.

[123] The NIST Cybersecurity Framework provides a robust sequence of control activities in response to and recovery from detected security incidents. First, in the Information Protection Processes and Procedures category, "[r]esponse plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed" and "[r]esponse and recovery plans are tested."[309] Second, under the Detect function, the Anomalies and Events category of activities help ensure that "[a]nomalous activity is detected in a timely manner and the potential impact of events is understood."[310] Third, in the Respond function, categories of activities include Response Planning ("[r]esponse processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events"), Communications ("[r]esponse activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies"), Analysis ("[a]nalysis is conducted to ensure adequate response and support recovery activities"), Mitigation ("[a]ctivities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident"), and Improvements ("[o]rganizational response activities are improved by incorporating lessons learned from current and previous detection/response activities").[311] Finally, under the Recover function, activities include Recovery Planning ("[r]ecovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events"); Improvements ("[r]ecovery planning and processes are improved by incorporating lessons learned into future activities"); and Communications ("[r]estoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs [computer security incident response teams], and vendors").[312]

[309] Cybersecurity Framework, *supra* note 134, at 28.

[310] *Id.* at 30.

[311] *See id.* at 33–34.

F. Adjust

An Organization Should Periodically Review and Update its Policies and Controls for the Security of Protected Information

[124] An organization's operations, activities, and systems change over time, as do its information security risks. An organization should therefore periodically evaluate the effectiveness of its information security program and make timely changes consistent with the organization's legal requirements, obligations to third-parties, and strategic objectives.

[125] Legal requirements for information security programs uniformly require review and updating of such programs on a periodic basis, or whenever changed circumstances indicate that such updating is needed.[313]

---

[312] *See id.* at 34–35.

[313] *See, e.g.*, 12 C.F.R. pt. 30, app. B(III)(E) (2014). The Interagency Guidelines Establishing Information Security Standards under Gramm-Leach-Bliley state that:

> Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

Id. The FTC Safeguards Rule under Gramm-Leach-Bliley requires an organization to:

> Evaluate and adjust your information security program in light of the results of the testing and monitoring required . . . any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.4(e) (2014).

[126] In its enforcement actions under the Gramm-Leach-Bliley Safeguards Rule, the FTC has alleged that companies failed to evaluate and adjust their information security programs in light of known or identified risks.[314] The FTC has also found fault with the alleged failure of companies to "implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents."[315]

[127] FTC Consent Orders commonly require

The HIPAA Security Rule requires covered entities and business associates to "[p]erform a periodic technical and nontechnical evaluation . . . in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart." 45 C.F.R. § 164.308(a)(8) (2013). Covered entities and business associates must also review and modify their security measures "as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures . . . ." 45 C.F.R. § 164.306(e) (2013); *see also* 201 MASS. CODE REGS. 17.03(2)(h), (i) (2014) (requiring upgrading of information safeguards as necessary to limit risks, and "[r]eviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.") (Massachusetts PII Protection Standards); OR. REV. STAT. ANN. § 646A.622(2)(d)(A)(vi) (West 2011) (information security program deemed compliant if, among other matters, the organization "[a]djusts the security program in light of business changes or new circumstances . . . .") (Oregon PII Safeguards Statute).

[314] *See, e.g.*, Complaint at 4, *In re* ACRAnet, Inc., No. C-4331 (F.T.C. Aug. 17, 2011) [hereinafter ACRAnet Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110809acranetcmpt.pdf, *archived at* http://perma.cc/37X2-P749; James B. Nutter & Co. Complaint at 3; Nations Title Agency Complaint at 3; SettlementOne Credit & Sackett National Holdings Complaint at 4.

[315] HTC America Complaint at 2; *see also* Fandango Complaint at 4 ("[f]ailing to maintain an adequate process for receiving and addressing security vulnerability reports from third parties.").

> The evaluation and adjustment of the information security program in light of the results of the testing and monitoring required [by the consent order] . . . , any material changes to operations or business arrangements, or any other circumstances that Defendant knows or has reason to know may have material impact on the effectiveness of the information security program.[316]

[128] ISO 27002 provides that "[t]he policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continued suitability, adequacy and effectiveness."[317]

[129] The NIST Cybersecurity Framework incorporates the concept of continuous improvement in its various functions, including Protection ("[p]rotection processes are continuously improved"); Detection ("[d]etection processes are continuously improved"); Response ("[o]rganizational response activities are improved by incorporating lessons learned from current and previous detection/response activities."); and Recovery ("[r]ecovery planning and processes are improved by incorporating lessons learned into future activities.").[318]

III. CONCLUSION

[130] Litigants and practitioners are vigorously contesting the FTC's authority to enforce information security under Section 5 of the FTC Act, in the absence of an underlying regulatory scheme.[319] This article takes no

[316] *See, e.g.*, Accretive Health Order at 3; *see also* consent orders cited *supra* note 43 (for similar language in consent orders under Gramm-Leach-Bliley); consent orders cited *supra* note 45 (for language in consent orders under COPPA), *and* consent orders cited *supra* notes 51, 52, and 54 (for similar language in consent orders under FTC Act § 5).

[317] ISO 27002, *supra* note 5, at § 5.1.2.

[318] Cybersecurity Framework, *supra* note 134, at 27, 32, 34–35.

position on the validity of such challenges, or on the application of the fair notice doctrine to the FTC's enforcement activities under Section 5. But, there is an irony here. Such challenges seem grounded in the notion that sector-specific information security laws provide clear-cut prescriptions for information security programs and controls in stark contrast to the absence of such specific data security standards under Section 5.

[131] This contrast is largely illusory. As explored in Section II, the concept of reasonableness pervades virtually every expression of United States' information security law, from the most granular standards, such as the HIPAA Security Rule, to the FTC's COPPA regulations, the U.S.-EU Safe Harbor's Security Principle, and numerous state laws, which simply require "reasonable" procedures and practices for safeguarding protected information without further elaboration. The fundamental question, therefore, is what constitutes a reasonable information security program?

[132] The six elements of a reasonable information security program set forth in this article are the common threads that emerge from federal and state information security laws. These elements are also supported by other authoritative sources, including ISO 27002 and the NIST Cybersecurity Framework. They allow flexibility regarding the diverse security circumstances of different organizations, for they should be addressed in a manner consistent with applicable legal requirements and the organization's obligations to third-parties and strategic approach to risk management. But most importantly, these six elements can hopefully serve as common ground for organizations in establishing reasonable safeguards, in a perilous world for information.

[319] *See, e.g.*, Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 674 (2013); *see also* Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 6–10, FTC v. Wyndham Worldwide Corp., No. 12-cv-01365-PHX-PGR (D. Ariz. Aug. 27, 2012).