HUSCH BLACKWELL

FTC Enforcement of Data Security

By Peter Sloan and Cordero Delgadillo

WHITE PAPER

MAY 18, 2015

Prudent organizations are mindful of the FTC's enforcement positions when establishing and adapting their information safeguards, in an evolving, volatile threat environment.

For more than a decade the Federal Trade Commission has quietly enforced data security in administrative proceedings against U.S. companies large and small, across a wide range of industries. Until recently, no organization has vigorously pushed back.[1] Instead, from CVS Caremark to Credit Karma, from Facebook to Franklin's Budget Car Sales, and from Lifelock to Life is Good, Inc., companies have agreed to consent orders imposing up to 20 years of FTC oversight for their data security programs.

This record of administrative complaints and consent orders from over 50 FTC data security enforcement matters provides a wealth of information on what the FTC considers adequate data security – lessons to be ignored at an organization's peril.

The FTC's Authority to Enforce Data Security

The FTC has enforcement authority under several U.S. laws that require security safeguards for protected information, including the Gramm-Leach-Bliley Act (GLBA),[2] the Fair and Accurate Credit Transactions Act (FACTA),[3] and the Children's Online Privacy Protection Act (COPPA).[4]

The FTC also has enforcement authority against companies that have Safe Harbor status under the U.S.-EU Safe Harbor Framework, which allows such companies to participate in the transfer of personal data protected by the European Commission's Directive on Data Protection.[5]

Since 2002, however, the majority of the FTC's data 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."[6] Under Section 5, the FTC enforces information security through one or a combination of two prohibitions:

- **Deception:** 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.[7]
- **Unfairness:** The FTC may instead pursue a company under the unfairness prong of Section 5, without relying on any misrepresentation about information security.[8] In an unfairness claim, however, the FTC must also allege 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."[9]

In fifteen concluded enforcement matters concluded since 2002, the FTC has pursued companies for inadequate data security solely under a Section 5 deception theory, with no companion claims under GLBA, FACTA, or COPPA, and therefore with no underlying regulatory standards with prescribed safeguards.[10] In each of these matters the 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.[11]

During the same thirteen year period, the FTC alleged Section 5 data security violations under a combination of deception and unfairness theories in twelve concluded enforcement matters. 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.[12]

And in 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 based neither on specific regulatory standards nor on allegedly deceptive representations about 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.[13] The 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.[14]

This white paper explores the FTC's enforcement positions on data security, categorizing them under six fundamental elements of an organization's information security program: Identify, Assess, Safeguard, Contract, Respond, and Adjust.

Six Elements of a Reasonable Information Security Program

FTC data security enforcement aligns with the following six elements of a reasonable information security program, which are derived from U.S. federal and state legal requirements and also voluntary standards including ISO 27002 and the NIST Framework for Improving Critical Infrastructure Cybersecurity.[15]

Identify - An organization should identify the types of information in its possession, custody, or control for which it will establish security safeguards ("Protected Information").

Assess - An organization should assess anticipated threats, vulnerabilities, and risks to the security of Protected Information.

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.

Contract - An organization should address the security of Protected Information in its third-party relationships.

Respond - An organization should respond to detected breaches of the security of Protected Information.

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

I. Identify

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.[16]

Information subject to FTC data security enforcement includes data protected under GLBA, FACTA, COPPA, and also protected information in the FTC's enforcement actions under Section 5 of the FTC Act.

A. GLBA Customer Information

Under GLBA, financial institutions must protect the security and confidentiality of their customers' nonpublic personal information,[17] 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."[18]

B. FACTA Consumer Information

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 . . . ." Consumers are individuals,[20] 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]."[21]

C. COPPA Personal Information

Regulations under COPPA require safeguards for personal information that covered websites or online services collect from children.[22] Children are individuals under the age of thirteen,[23] 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].[24]

D. FTC Act Section 5 Protected Information

In FTC enforcement actions under Section 5 of the FTC Act, not involving enforcement of GLBA, FACTA, or COPPA, the most common type of protected information is nonpublic personal information conducive to identity theft, including consumer names, physical and email 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-issued identification numbers.[25] These categories of information are familiar territory under state laws protecting personally identifiable information (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;[26] physician names, insurance numbers, diagnosis codes, and medical visit types;[27] 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;[28] prescription medications and dosages, prescribing physician names, addresses, and telephone numbers, health insurer names, and insurance account and policy numbers;[29] genetic information;[30] medical histories, health care providers' examination notes, medications, and psychiatric notes;[31] 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).[32] These categories of health-related personal information are comparable to protected health information (PHI) under HIPAA.

Other FTC enforcement actions under Section 5 have focused on safeguards for nonpublic consumer identification information from credit reporting agencies[33] and credit report information generally;[34] information similar to that protected under FACTA.

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;[35] nonpublic social network profile information;[36] and nonpublic smart phone data, including text message content, GPS location data, web browsing and media viewing history, phone numbers of users and contacts, and numeric keys pressed.[37] 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 company engaged in deceptive conduct by misrepresenting that the information would remain private or be safeguarded.

The FTC, under a Section 5 deception 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.[38]

In its enforcement action against Eli Lily, the FTC's Section 5 deception claim focused simply on the names and email addresses contained within a single group email sent to 669 persons.[39] 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.[40]

In 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.[41] Notably, live video feeds are not specified as 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.[42] 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.[43]

II. Assess

Once an organization determines the types of information to be safeguarded, it should then assess anticipated threats, vulnerabilities, and risks to the security of that information. Such an assessment is crucial to help the organization understand its information security environment and to identify its priorities in developing an information security program.

The FTC Safeguards Rule under GLBA 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, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks."[44] 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.[45]

FTC enforcement actions under GLBA commonly allege a failure to "identify reasonably foreseeable internal and external risks to customer information."[46] The FTC has also taken the position in enforcement actions under FTC Act Section 5 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.[47] Additionally, FTC consent orders routinely require that 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."[48]

III. Safeguard

Informed by its risk assessment for the types of information to be safeguarded, an organization should establish and maintain appropriate policies and controls to address the identified threats, vulnerabilities, and risks to the security of such information.[49] 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.

A. Information Security Policy

An organization should have a policy that addresses 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. Legal requirements for information security commonly require a written information security program to address identified risks,[50] and several such laws require a designation of who is responsible for implementing and maintaining the program.[51]

In its enforcement proceedings under GLBA and FACTA, the FTC has frequently focused on the respondent's failure to develop a comprehensive written information security program.[52] The FTC has also taken the position under FTC Act Section 5 that the failure to "implement reasonable policies and procedures to protect the security of consumers' personal information collected and maintained by respondents" is an unfair and deceptive trade practice,[53] 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.[54]

FTC Consent Orders under the authority of GLBA,[55] COPPA,[56] and FTC Act Section 5 [57] commonly require the respondent to establish a written, comprehensive information security program. Such orders also require "[t]he designation of an employee or employees to coordinate and be accountable for the information security program . . . ."[58]

B. Controls

The FTC has taken the position that some security safeguards are to be expected due to their ready availability, low cost, and common use.

An organization may appropriately establish a variety of administrative, physical, and technical controls to address its information security risks. Different organizations in different industries and circumstances will have different security risks, and so the selection of appropriate controls will vary between organizations.

Most information security laws explicitly allow for flexibility in establishing security controls for information, taking into consideration such matters as the organization's available resources and the cost of security measures. But the FTC has taken the position that some security safeguards are to be expected due to their ready availability, 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.[59]

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.[60] Further, the FTC has deemed limiting access to computer networks through wireless access points to be a "readily available" security measure.[61]

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;[62]
- commonly accepted and well known secure programming practices, including practices described in guidance documentation for software manufactures and developers;[63]
- readily available security measures to prevent unauthorized access, including installing patches and critical updates to the company's network;[64]
- readily available, low-cost measures to address risks of a software program collecting sensitive information in an unauthorized manner;[65] and
- commonly used safeguards for requiring strong user passwords.[66]

Below are nine categories of security controls that feature prominently in FTC data security enforcement. These information safeguards are also commonly referenced in data security legal requirements and voluntary security standards.

FTC Data Security Controls

These nine categories of data security controls are addressed in FTC data security enforcement proceedings:

- **system access**
- **physical access**
- **encryption**
- **transmission security**
- **mobile device and portable media security**
- **system change management**
- **monitoring and detection**
- **retention**
- **disposal**

1. System Access Controls

System access controls are designed to help ensure that only authorized individuals have access to systems containing protected information. Also, these controls usually feature mechanisms to authenticate the identity of the individual seeking access.[67]

System access controls are commonly required under legal requirements for information security programs,[68] 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;[69] failure to require periodic change of passwords or to prohibit use of the same password across multiple applications and programs;[70] failure to suspend users after a reasonable number of unsuccessful login attempts;[71] and the practice of storing passwords or other network user credentials in clear readable text.[72]

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.[73] 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;[74] 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;[75] and the failure in general to restrict access to those individuals with a valid need for the protected information.[76]

2. Physical Access Controls

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.[77] Such physical controls are commonly referenced in information security legal requirements.[78]

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."[79]

3. Encryption

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").

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.[80] In at least sixteen enforcement matters the FTC has pursued companies under FTC Act Section 5 for storing protected information; usually card holder data, in clear readable text.[81] Most of these Section 5 enforcement actions for failure to encrypt data-at-rest were deception claims based on alleged representations that protected information stored on the company's systems would be encrypted or otherwise secure.[82]
But in 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.[83]

4. Transmission Security Controls

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.

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.[84]

5. Mobile Device & Portable Media Controls

Safeguard controls can be applied to address security risks for protected information stored in mobile devices, such as laptops and smartphones, and in portable storage media.[85] 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.

Mobile device and portable media security has been central to several 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.[86] 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.[87]

Similarly, 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.[88] 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.[89] As 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."[90] 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 . . . ."[91]

6. System Change Management Controls

At most organizations, computer applications and systems are in a 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.

Change management failures have 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 development of a smartphone application, but the security feature was not re-enabled before the application was launched to consumers.[92] 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.[93] 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.[94] The FTC alleged that respondents failed to "implement appropriate checks and controls on the process of writing and revising Web applications . . . ."[95]

7. Monitoring & Detection Controls

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.[96] 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.[97]

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.[98] In *Cbr Systems, Inc.,* the FTC alleged that the respondent:

> 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.[99]

8. Retention Controls

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.[100] 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.

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.[101]

9. Disposal Controls

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,[102] as well as the destruction of protected information in hard copy media.

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.[103] The FTC's FACTA Disposal Rule requires 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."[104]

The FTC has entered into consent orders with several companies for failing to comply with disposal safeguards under FACTA and GLBA.[105] 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.[106]

C. Training

An organization should use training and other awareness-building efforts to help ensure that its employees understand their responsibilities regarding information security.[107] Training is commonly referenced in legal requirements for information security programs.[108] Inadequate training is also frequently cited by the FTC in

its enforcement proceedings, including employee guidance and training on such matters as privacy and information security generally;[109] the prevention of unauthorized disclosure of personal information;[110] proper design, review, and testing of security for applications and software, for employees with those responsibilities;[111] secure access from remote locations;[112] proper response to security incidents;[113] and secure disposal.[114]

D. Testing

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.

Testing and monitoring of security controls feature prominently in legal requirements for information security programs.[115] FTC consent orders commonly require "regular testing and monitoring of the effectiveness of the safeguards' key controls, systems, and procedures."[116] 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."[117]

Inadequate contracting and oversight for service providers with protected information access can constitute an unfair and deceptive trade practice under FTC Act Section 5.

IV. Contract

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.[118] 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.

Legal requirements for information security commonly mandate that the safeguarding of protected information be addressed in third party relationships. Various safeguard rules promulgated under GLBA require oversight of service provider arrangements in three phases 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.[119]

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 to dispose of material, specifically identified as consumer information, in a manner consistent with this rule."[120]

Under its GLBA 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.[121] 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 FTC Act Section 5.

For example, in *GeneLink, Inc.* and *foruTM 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™ permitted their service providers to access collected personal information in order to maintain GeneLink and foru™'s customer relationship databases, fulfill customer orders, and develop related applications. [22] According to the FTC, GeneLink and foru™ "[f]ailed to require by contract that service providers implement and maintain appropriate safeguards for consumers' personal information"[123] 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." The resulting consent decrees required GeneLink and foru™ to develop and use "reasonable steps to select and retain service providers capable of appropriately safeguarding Personal Information received" from the companies, and also compelled them to require "service providers by contract to implement and maintain appropriate safeguards . . . ."[124]

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."[125] Similarly, in *Credit Karma,* the FTC alleged it was a deceptive and unfair practice under FTC Act Section 5 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.[126]

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."[127]

V. Respond

Most FTC data enforcement proceedings have followed one or more incidents of hacking, theft, or other unauthorized disclosure of protected information.

Most FTC data enforcement proceedings have followed one or more incidents of hacking, theft, or other unauthorized disclosure of protected information. 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.[128] Legal requirements for information security programs commonly require that covered organizations have the capability to respond when unauthorized access to protected information occurs.[129] And numerous laws require breach notification to affected individuals and, in certain circumstances, to governmental and other authorities if a breach occurs to protected information.[130]

VI. Adjust

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.

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.[131]

In its enforcement actions under the GLBA Safeguards Rule, the FTC has alleged that companies failed to evaluate and adjust their information security programs in light of known or identified risks.[132] 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."[133]

FTC Consent Orders routinely require "[t]he 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."[134]

Conclusion

For over a decade the FTC has enforced data security under both specific regulatory regimes and also Section 5 of the FTC Act. While litigants and some practitioners are currently contesting the FTC's authority to enforce reasonable security under the unfairness prong of Section 5,[135] it nevertheless seems clear that the FTC will continue to have a significant role in shaping expectations for data security generally.

The accumulated record from over 50 FTC proceedings, which has been dubbed part of a "new common law of privacy,"[136] provides extensive insight into what the FTC considers to be adequate data security. Prudent organizations will be mindful of the FTC's enforcement positions when establishing and adapting their information safeguards, in an evolving, volatile threat environment.

---

[1] In 2012, the FTC filed a complaint against Wyndham Worldwide Corporation and several subsidiaries ("Wyndham") in the Federal District Court of Arizona. Similar to LabMD, Wyndham challenged the FTC's enforcement authority under the unfairness prong of § 5 of the FTC Act. Wyndham filed a motion to dismiss, arguing that the FTC does not have authority to regulate data security under FTC Act § 5 and that the FTC failed to provide adequate notice of reasonable data security practices. The lower court denied Wyndham's motion, but the issues are now pending in the Third Circuit Court of Appeals on an interlocutory appeal. *See generally* Case Timeline, Wyndham Worldwide Corp., FTC File No. 1023142, Fed. Trade Comm'n, https://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation (last updated Mar. 27, 2015).

In 2013, LabMD challenged the FTC's 2010 administrative proceeding against the company, claiming that the FTC exceeded its authority under the unfairness prong of FTC Act § 5 by attempting to regulate LabMD, a HIPAA Covered Entity. LabMD's motion to dismiss the administrative complaint was denied by the lower federal court, and its appeal to the Eleventh Circuit was dismissed for lack of a final administrative decision, thereby requiring LabMD to complete the ongoing administrative process. *See generally* Case Timeline, In re LabMD, FTC File No. 102 3099, Fed. Trade Comm'n, https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter (last updated Apr. 30, 2015).

[2] *See* 15 U.S.C. § 6805(a)(7). GLBA requires that financial institution regulators establish standards for "administrative, technical, and physical safeguards" for "the security and confidentiality of customer records and information." 15 U.S.C. §§ 6801(b). The FTC standards for safeguarding customer information, applicable to those financial institutions not subject to the jurisdiction of other functional regulators, contain "standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information." 16 C.F.R. § 314.1(a).

[3] *See* 15 U.S.C. § 1681w(a)(1). FACTA requires that financial institution regulators promulgate rules requiring the proper disposal of customer information derived from consumer reports for a business purpose. 15 U.S.C. § 1681w(a)(1). The FTC's Disposal Rule promulgated under FACTA requires 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." 16 C.F.R. § 682.3(a).

[4] *See* 15 U.S.C. § 6502(b)(1). COPPA requires the Federal Trade Commission 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." 15 U.S.C. § 6502(b)(1)(D). The FTC's COPPA Rule succinctly provides that such operators "must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children." 16 C.F.R. § 312.8.

[5] *See* U.S.- EU Safe Harbor Overview, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018476.asp. 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. 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. 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." Id.

[6] 15 U.S.C. § 45(a)(1).

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

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

[9] 15 U.S.C. § 45(n). See, e.g., Dave & Buster's Complaint at 3.

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

http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrcmpt.pdf; Complaint at 5–6, In re Credit Karma, Inc., No. C-4480 (F.T.C. Aug. 13, 2014) [Credit Karma Complaint], http://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf; Complaint at 3, In re Eli Lily & Co., No. C-4047 (F.T.C. May 8, 2002) [Eli Lily Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillycmp.htm; Complaint at 5, In re Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014) [Fandango Complaint], http://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf; Complaint at 3, In re Genica Corp., No. C-4252 (F.T.C. Mar. 16, 2009) [Genica Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090320genicacmpt.pdf; Complaint at 3, In re Guess?, Inc., No. C-4091 (F.T.C. July 30, 2003) [Guess Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2003/08/guesscomp.pdf; Complaint at 3, In re Guidance Software, Inc., No. C-4187 (F.T.C. Mar. 30, 2007) [Guidance Software Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2007/04/0623057complaint.pdf; Complaint at 3, In re Life is Good, Inc., No. C-4218 (F.T.C. Apr. 16, 2008) [Life is Good Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2008/04/080418complaint.pdf; Complaint at 5, In re Microsoft Corp., No. C-4069 (F.T.C. Dec. 20, 2002) [Microsoft Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2002/08/microsoftcmp.pdf; Complaint at 4, In re MTS, Inc. & Tower Direct, LLC, No. C-4110 (F.T.C. May 28, 2004) [MTS and Tower Direct Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2004/06/040602comp0323209.pdf; Complaint at 5-6, 8, In re Myspace LLC, No. C-4369 (F.T.C. Aug. 30, 2012) [Myspace Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacecmpt.pdf (also alleging misrepresentations regarding U.S. Safe Harbor adherence); Complaint at 4, In re Petco Animal Supplies, Inc., No. C-4133 (F.T.C. Mar. 4, 2004) [Petco Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2005/03/050308comp0323221.pdf; Twitter Complaint at 5.

[11] *See* Consent Order at 5, FTC v. LifeLock, Inc., No. 072-3069 (D. Ariz. Mar. 9, 2010) [LifeLock Order], http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockstip.pdf; Consent Order at 9–10, United States v. ValueClick, Inc., No. CV08-01711 MMM (RZx) (C.D. Cal. Mar. 17, 2008) [ValueClick Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317judgment.pdf; Consent Order at 3, In re Cbr Systems, Inc., No. C-4400 (F.T.C. April 29, 2013) [Cbr Systems Order], http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrdo.pdf; Consent Order at 3, In re Credit Karma, Inc., No. C-4480 (F.T.C. Aug. 13, 2014) [Credit Karma Order], http://www.ftc.gov/system/files/documents/cases/1408creditkarmado.pdf; Consent Order at II., In re Eli Lily & Co., No. C-4047 (F.T.C. May 8, 2002) [Eli Lily Order], http://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillydo.htm; Consent Order at 3, In re Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014) [Fandango Order], http://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf; Consent Order at 3, In re Genica Corp., No. C-4252 (F.T.C. Mar. 16, 2009) [Genica Order], http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090320genicado.pdf; Consent Order at 3, In re Guess?, Inc., No. C-4091 (F.T.C. July 30, 2003) [Guess Order], http://www.ftc.gov/sites/default/files/documents/cases/2003/08/guessdo.pdf; Consent Order at 2–3, In re Guidance Software, Inc., No. C-4187 (F.T.C. Mar. 30, 2007) [Guidance Software Order], http://www.ftc.gov/sites/default/files/documents/cases/2007/04/0623057do.pdf; Consent Order at 3, In re Life is Good, Inc., No. C-4218 (F.T.C. Apr. 16, 2008) [Life is Good Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/04/080418do.pdf; Consent Order at 2–3, In re Microsoft Corp., No. C-4069 (F.T.C. Dec. 20, 2002) [Microsoft Order], http://www.ftc.gov/sites/default/files/documents/cases/2002/12/microsoftdecision.pdf; Consent Order at 3, In re MTS, Inc., & Tower Direct, LLC, No. C-4110 (F.T.C. May 28, 2004) [MTS and Tower Direct Order], http://www.ftc.gov/sites/default/files/documents/cases/2004/06/040602do0323209.pdf; Consent Order at 3, In re Myspace LLC, No. C-4369 (F.T.C. Aug. 30, 2012) [Myspace Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacedo.pdf; Consent Order at II., In re Petco Animal Supplies, Inc., No. C-4133 (F.T.C. Mar. 4, 2005) [Petco Order], http://www.ftc.gov/sites/default/files/documents/cases/2005/03/050308do0323221.pdf; Consent Order at 3, In re Twitter, Inc., No. C-4316 (F.T.C. Mar. 2, 2014) [Twitter Order], http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf.

[12] *See* Consent Order at 3, In re Ceridian Corp., No. C-4325 (F.T.C. June 8, 2011) [Ceridian Corp. Order], http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110615ceridiando.pdf; Consent Order at 7, In re Compete, Inc., No. C-4384 (F.T.C. Feb. 20, 2013) [Compete Order], http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competedo.pdf; Consent Order at 3, In re CVS Caremark Corp., No. C-4259 (F.T.C. June 18, 2009) [CVS Order], http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvsdo.pdf; Consent Order at 5, In re Facebook, LLC, No. C-4365 (F.T.C. July 27, 2012) [Facebook Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; Consent Order at 7, In re GeneLink, Inc., No. C-4456 (F.T.C. May 8, 2014) [GeneLink Order], http://www.ftc.gov/system/files/documents/cases/140512genelinkdo_0.pdf; Consent Order at 3, In re GMR Transcription Services, Inc., No. C-4482 (F.T.C. Aug. 14, 2014) [GMR Transcription Services Order], http://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf; Consent Order at 3, In re HTC America, Inc., No. C-4406 (F.T.C. June 25, 2013) [HTC America Order], http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf; Consent Order at 3, In re Lookout Servs., Inc., No. C-4326 (F.T.C. June15, 2011) [Lookout Services Order], http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110615lookoutdo.pdf; Consent Order at 3, In re Rite Aid, Corp., No. C-4308 (F.T.C. Nov. 12, 2010) [Rite Aid Order], http://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaiddo.pdf; Consent Order at 4, In re TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014) [TRENDnet Order], http://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf; Consent Order at 6, In re Upromise, Inc., No. C-4351 (F.T.C. Mar. 27, 2012) [Upromise Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisedo.pdf.

[13] *See*, *e.g.*, Complaint at 2, In re Accretive Health, Inc., No. C-4432 (F.T.C. Feb. 5, 2014) [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."); Complaint at 2, In re BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005) [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."); Complaint at 2, In re CardSystems Solutions, Inc., No. C-4168 (F.T.C. Sept. 5, 2006) [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."); 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) [DSW Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2005/12/051201comp0523096.pdf ("[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."); Complaint at 2, In re EPN, Inc., No. C-4370 (F.T.C. Oct. 3, 2012) [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."); Complaint at 3, In re Reed Elsevier, Inc., No. C-4226 (F.T.C. July 29, 2008) [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 . . . ."); Complaint at 2, In re TJX Cos., No. C-4227 (F.T.C. July 29, 2008) [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."). 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) [LabMD Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.

[14] *See* Consent Order at 2–3, In re Accretive Health, Inc., No. C-4432 (F.T.C. Feb. 5, 2014) [Accretive Health Order], http://www.ftc.gov/system/files/documents/cases/140224accretivehealthdo.pdf; Consent Order at 2–3, In re BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005) [BJ's Wholesale Club Order], http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305do0423160.pdf; Consent Order at 3, In re Cardsystems Solutions, Inc., No. C-4168 (F.T.C. Sept. 5, 2006) [Cardsystems Solutions Order], http://www.ftc.gov/sites/default/files/documents/cases/2006/09/0523148cardsystemsdo.pdf; Consent Order at 2–3, In re Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010) [Dave & Buster's Order], http://www.ftc.gov/sites/default/files/documents/cases/2010/06/100608davebustersdo.pdf; Consent Order at 2–3, In re DSW Inc., No. C-4157 (F.T.C. Mar. 7, 2006) [DSW Order], http://www.ftc.gov/sites/default/files/documents/cases/2006/03/0523096c4157dswdecisionandorder.pdf; Consent Order at 2–3, In re EPN, Inc., No. C-4370 (F.T.C. Oct. 3, 2012) [EPN Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epndo.pdf; Consent Order at 3–4, In re Reed Elsevier, Inc., No. C-4226 (F.T.C. July 29, 2008) [Reed Elsevier Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reeddo.pdf; Consent Order at 2–3, In re TJX Cos., No. C-4227 (F.T.C. July 29, 2008) [TJX Cos. Order], http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxdo.pdf.

[15] *See* Peter Sloan, The Reasonable Information Security Program, 21 RICH. J.L. & Tech. 2 (2014), http://jolt.richmond.edu/v21i1/article2.pdf.

[16] 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 [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.

[17] *See* 15 U.S.C. § 6801(a).

[18] 15 U.S.C. § 6809(4).

[19] 15 U.S.C. § 1681w(a)(1). See also 16 C.F.R. § 682.3(a).

[20] 15 U.S.C. § 1681a(c).

[21] 15 U.S.C. §§ 1681a(d)(1)(A)–(C).

[22] *See* 15 U.S.C. § 6502(b)(1)(D).

[23] 15 U.S.C. § 6501(1).

[24]15 U.S.C. § 6501(8). 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 (defining "personal information").

[25] *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), [CVS Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf; Dave & Buster's Complaint at 2; DSW Complaint at 1, 3; EPN Complaint at 1, 3; Fandango Complaint at 2, 4–5; GeneLink and foruTM 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) [GMR Transcription Services Complaint], http://www.ftc.gov/system/files/documents/cases/140203gmrcmpt.pdf; 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; 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), [Rite Aid Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaidcmpt.pdf; TJX Complaint at 2–3; Upromise Complaint at 3, 6.

[26] Accretive Health Complaint at 2.

[27] EPN Complaint at 1.

[28] LabMD Complaint at 2.

[29] CVS Complaint at 2. See also Rite Aid Complaint at 1–2.

[30] GeneLink and foruTM Complaint at 12.

[31] GMR Transcription Services Complaint at 2.

[32] Cbr Systems Complaint at 1–2.

[33] Reed Elsevier Complaint at 2.

[34] Credit Karma Complaint at 1–2.

[35] Compete Complaint at 3. See also Upromise Complaint at 2.

[36] Complaint at 2–3, Facebook, Inc., No. C-4365, (F.T.C. Aug. 10, 2012) [Facebook Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf. See also Myspace Complaint at 1–2; Twitter Complaint at 1–2.

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

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

[39] Eli Lily Complaint at 3.

[40] *Id.*

[41] Complaint at 5, TRENDnet, Inc., No. C-4426, (F.T.C. Feb. 7, 2014) [TRENDnet Complaint], http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[42] *See id.* at 3–4.

[43] *Id.* at 6.

[44] 16 C.F.R. § 314.4(b) (2014).

[45] *Id.*

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

[47] *See* GeneLink and foruTM 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.").

[48] *See* Accretive Health Order at 3. *See generally* 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).

[49] FTC Consent Orders commonly require "[t]he design and implementation of reasonable safeguards to control the risks identified through risk assessment . . . ." See, e.g., Accretive Health Order at 3.

[50] *See* 16 C.F.R. § 314.3(a) ("[y]ou shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts . . . .").

[51] Organizations subject to the FTC Safeguards Rule must "[d]esignate an employee or employees to coordinate [the] information security program." 16 C.F.R. § 314.4(a).

[52] *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; Sunbelt Lending Complaint at 2–3.

[53] GeneLink and foruTM Complaint at 13–14.

[54] LabMD Complaint at 3.

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

[56] *See* Consent Order at 5, 8, In re RockYou, Inc., No. 12-CV-1487 (F.T.C. Mar. 27, 2012) [RockYou Order], http://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf; Consent Order at 12–13, United States v. Path, Inc., No. 13-CV-00448-RS (N.D. Cal. Feb. 8, 2013) [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").

[57] *See* notes 11, 12, & 14.

[58] *See*, *e.g.*, Accretive Health Order at 3.

[59] *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; 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) [Nations Title Agency Complaint], http://www.ftc.gov/sites/default/files/documents cases/2006/06/0523117nationstitle_complaint.pdf; Reed Elsevier Complaint at 4.

[60] *See*, *e.g.*, Complaint at 10, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012) [Wyndham Worldwide Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf; Dave & Buster's Complaint at 2; Genica Complaint at 2–3; TJX Cos. Complaint at 2.

[61] *See*, *e.g.*, Dave & Buster's Complaint at 2; Complaint at 13, In re GeneLink, Inc., & foruTM Int'l Corp., No. C-4456 (F.T.C. May 8, 2014) [GeneLink and foruTM Complaint], http://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf; Life is Good Complaint at 2; TJX Cos. Complaint at 2.

[62] *See*, *e.g.*, Complaint at 4–5, In re Compete, Inc., No. C-4384 (F.T.C. Feb. 20, 2013) [Compete Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf.

[63] Complaint at 2, In re HTC America, Inc., No. C-4406 (F.T.C. June 25, 2013) [HTC America Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf.

[64] LifeLock Complaint at 10.

[65] Complaint at 4, In re Upromise, Inc., No. C-4351 (F.T.C. Mar. 27, 2012) [Upromise Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf.

[66] Wyndham Worldwide Complaint at 11.

[67] *See* FTC Business Guidance 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).

[68] *See* 16 C.F.R. §§ 314.4(b)–(c) (requirement to implement information safeguards to control identified risks, including the "unauthorized disclosure, misuse, alteration, destruction or other compromise" of protected information).

[69] *See* CardSystems Solutions Complaint at 2; 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.

[70] *See* LabMD Complaint, at 3; LifeLock Complaint at 10; Lookout Services Complaint at 2; Reed Elsevier Complaint at 3; TJX Complaint at 2; Twitter Complaint at 4.

[71] *See* LifeLock Complaint at 10; Lookout Services Complaint at 2; Reed Elsevier Complaint at 3; Twitter Complaint at 4.

[72] *See* Guidance Software Complaint at 2; Reed Elsevier Complaint at 3; Twitter Complaint at 4.

[73] *See* BJ's Wholesale Club Complaint at 2; Reed Elsevier Complaint at 3.

[74] *See* Dave & Buster's Complaint at 2; Wyndham Worldwide Complaint at 10.

[75] *See* Complaint at 3, Equifax Info. Servs., LLC, No. C-4387 (F.T.C. Mar. 5, 2013) [Equifax Complaint] http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121010equifaxcmpt.pdf; Complaint at 9, United States v. ChoicePoint, Inc., No. 1:06-CV-0198-GET (N.D. Ga. Jan. 30, 2006) [ChoicePoint Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf; Complaint at 8, United States v. Rental Research Servs., Inc., No. 072-3228 (D. Minn. Mar. 5, 2009) [Rental Research Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrscmpt.pdf.

[76] *See* 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"); 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 foruTM 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).

[77] *See* FTC Business Guidance at 8–9 (Physical Security under the "Lock It" Principle).

[78] *See* 16 C.F.R. § 314.4(a).

[79] LifeLock Complaint at 10.

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

[81] *See* BJ's Wholesale Club Complaint at 2; 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) [RockYou Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf; TJX Complaint at 2; Twitter Complaint at 4.

[82] *See* Guidance Software Complaint at 2 ("we also do everything in our power to protect user-information off-line . . . ."); 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.").

[83] TJX Complaint at 2–3.

[84] *See* BJ's Wholesale Club Complaint at 2; 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; RockYou Complaint at 6; TJX Complaint at 2; Twitter Complaint at 4.

[85] *See* FTC Business Guidance at 13–14.

[86] Accretive Health Complaint at 2.

[87] *Id.*

[88] Cbr Systems Complaint at 3.

[89] *Id.*

[90] *Id.* at 2–3.

[91] *Id* at 3.

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

[93] HTC America Complaint at 5.

[94] MTS and Tower Direct Complaint at 3.

[95] *Id.* at 4.

[96] *See* FTC Business Guidance at 17 ("Detecting Breaches" under the "Lock It" Principle).

[97] *See* 16 C.F.R. §§ 314.4(b)(3), (c) (requiring information safeguards to control identified risks, including risks in "[d]etecting, preventing and responding to attacks, intrusions, or other systems failures.").

[98] *See* 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.

[99] Cbr Systems Complaint at 3.

[100] *See* FTC Business Guidance at 6–7 (referencing the "Scale Down" Principle and "keep[ing] only what you need for your business").

[101] *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.

[102] *See* FTC Business Guidance 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.").

[103] *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.").

[104] *See* note 3.

[105] *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) [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); Complaint at 5–6, United States v. PLS Financial Services, Inc., No. 1:12-cv-08334 (N.D. Ill. Oct. 17, 2012) [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); 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).

[106] *See* 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).

[107] *See* FTC Business Guidance at 17 ("Employee Training" under the "Lock It" Principle).

[108] *See* 16 C.F.R. § 314.4(b)(1), (c) (implement safeguards to control identified risks, including "[e]mployee training and management").

[109] *See* Eli Lily Complaint at 3; Nationwide Complaint at 3; Upromise Complaint at 4–5.

[110] EPN Complaint at 2.

[111] *See* MTS and Tower Direct Complaint at 3–4; TRENDnet Complaint at 4–5.

[112] Sunbelt Lending Complaint at 2.

[113] Goal Financial Complaint at 2.

[114] *See* CVS Complaint at 2; PLS Complaint at 5–6; Rite Aid Complaint at 2–3.

[115] *See* 16 C.F.R. § 314.4(c) ("[R]egularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures").

[116] Accretive Health Order at 3. See also sources cited in note 55 for such language in Consent Orders under Gramm-Leach-Bliley, sources in note 56 for such language in Consent Orders under COPPA, and sources in notes 11, 12, and 14 for such language in Consent Orders under FTC Act § 5.

[117] Accretive Health Order at 3; *see also* sources cited in notes 11, 12, 14, 55, & 56.

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

[119] See 16 C.F.R. §§ 314.4(d)(1) & (2).

[120] 16 C.F.R. § 682.3(b)(3) (2014). The Disposal Rule under FACTA provides examples of compliant due diligence, including "[r]eviewing 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.

[121] *See* 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).

[122] GeneLink and foruTM Complaint at 12.

[123] *Id.* at 13.

[124] *See* GeneLink Order at 7; Consent Order at 7, In re foruTM Int'l. Corp., No. C-4457 (F.T.C. May 8, 2014) [foruTM Order], http://www.ftc.gov/system/files/documents/cases/140512foruintdo.pdf.

[125] 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 . . . .").

[126] Credit Karma Complaint at 4.

[127] *See, e.g.*, Accretive Health Order at 3. *See also* notes 55 & 56 for similar language in consent orders under GLBA and COPPA and notes 11, 12, & 14 for similar language in Consent Orders under FTC Act § 5.

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

[129] *See* 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.").

[130] Though GLBA does not itself require breach notification, the rules of some financial institution regulators under GLBA require such notifications be made as part of the institution's mandated response programs. *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). 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.

[131] The FTC Safeguards Rule under GLBA requires organizations to "[e]valuate 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).

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

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

[134] *See, e.g.*, Accretive Health Order at 3. For similar language in Consent Orders under GLBA, see note 55; in Consent Orders under COPPA; see note 56; and in Consent Orders under FTC Act § 5 see notes 11, 12, & 14.

[135] *See* note 1. See also, 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).

[136] Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 COLUM. L. REV. 583 (2014).