1

Data Security Laws and Enforcement Actions

CHAPTER MENU

FTC Data Security 2
State Data Breach Notification Laws 36
State Data Security Laws 42
State Data Disposal Laws 49

The United States does not have a national law that prescribes specific data security standards for all industries. The only *federal* data security laws apply to companies that handle specific types of data, such as financial information or health records (discussed in Chapter 3). This comes as a surprise to many, and is frustrating to businesses that want to assure customers and regulators that they comply with all legal requirements, particularly for securing customers' personal information. Likewise, consumer advocates and privacy groups criticize the federal government for failing to enact data security requirements. In recent years, members of Congress and the White House have introduced legislation to set minimum data security standards, but, as of publication of this book, Congress has not enacted any such legislation.

Despite the lack of a statute that sets minimum data security requirements, the Federal Trade Commission aggressively polices data security. In recent years, the FTC has brought dozens of enforcement actions against companies that it believes have failed to take reasonable steps to secure the personal data of their customers. The FTC brings these actions under Section 5 of the FTC Act, a century-old law that was designed to protect consumers and competitors from unfair business practices. Although the law does not explicitly address cybersecurity, it is one of the primary tools that the government uses to bring enforcement actions against companies that failed to take adequate steps to protect consumer information.

This chapter provides an overview of data security requirements under Section 5 of the FTC Act, as well as under state data security laws and private tort claims.

Cybersecurity Law, First Edition. Jeff Kosseff.

Companion Website: www.wiley.com/go/kosseff/cybersecurity

First, we examine what the FTC considers to constitute "unfair" trade practices that violate Section 5. Next, we pay special attention to challenges to the FTC's cybersecurity authority. These challenges have been raised by two companies, Wyndham Worldwide Resorts and LabMD, and we conclude that, for now, it is largely accepted that the FTC has some authority to bring Section 5 complaints against companies that fail to adequately secure customer data. We then review how the FTC has applied that reasoning to cybersecurity, both in guidance and the dozens of complaints that it has filed against companies that allegedly failed to adequately secure personal information.

After reviewing the FTC's data security guidance and enforcement actions, we review the laws of 47 states and the District of Columbia that require companies to notify individuals, regulators, and credit bureaus after certain types of personal information are disclosed in a data breach. These laws are fairly complex, and the notification requirements vary by state. Failure to comply with the requirements in each of these statutes could lead to significant regulatory penalties and, in some cases, private lawsuits.

This chapter also provides an overview of the dozen state laws that require companies to implement reasonable data security programs and policies, and the 31 state laws that require companies to securely dispose of personal information.

1.1 FTC Data Security

The FTC is the closest thing that the U.S. federal government has to a centralized data security regulator. Many other agencies – including the Department of Health and Human Services, Education Department, and Federal Communications Commission – have jurisdiction to regulate privacy and data security for particular sectors. However, only the FTC has the authority to regulate companies in a wide range of sectors, provided that they engage in interstate commerce.

1.1.1 Overview of Section 5 of the FTC Act

The FTC claims its data security authority under Section 5 of the Federal Trade Commission Act,[1] which declares illegal "unfair or deceptive acts or practices in or affecting commerce."[2] The statute does not explicitly mention data security. The FTC commonly claims authority for data security enforcement actions under the "unfairness" prong of Section 5.

1 For the full text of § 5, *see* app. A.
2 15 U.S.C. § 45(a)(1).

Throughout the 1960s and 1970s, the FTC was criticized for broadly imposing its own value judgments when determining whether a practice is unfair. The Commission considered:

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise – whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; (3) whether it causes substantial injury to consumers (or competitors or other businessmen).[3]

This three-part test became known as the Cigarette Rule because the Commission articulated it as it was considering how to regulate cigarette advertising. Although the FTC did not frequently use this authority, the United States Supreme Court quoted it with approval in 1972, describing the three prongs as "the factors it considers in determining whether a practice that is neither in violation of the antitrust laws nor deceptive is nonetheless unfair."[4]

The FTC recognized the need to clarify the Cigarette Rule to focus more specifically on the injury to customers and benefits to society, rather than value judgments about whether the practice "offends public policy," is immoral, or unscrupulous. In 1980, the Commission issued the Unfairness Policy Statement, which the Commission wrote provides a "more detailed sense of both the definition and the limits of these criteria."[5] The statement articulates a new three-part test for unfairness claims: (1) "the injury must be substantial," (2) "the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces," and (3) "the injury must be one which consumers could not reasonably have avoided."[6]

In 1994, Congress amended the FTC Act to codify the 1980 Unfairness Policy Statement into law, Section 5(n) of the FTC Act. The statute states that "unfair" practices are those that cause or are 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."[7] This has created a three-part test that the FTC (and courts) must conduct to assess a trade practice.

---

3 Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 16 C.F.R. 408, 29 Fed. Reg. 8344 (July 2, 1964).

4 FTC v. Sperry & Hutchinson Co., 405 U.S. 233 (1972).

5 FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984).

6 *Id.*

7 15 U.S.C. § 45(n).

First, has the trade practice caused or is likely to cause *substantial* injury to customers? In other words, a minor injury will not constitute an unfair trade practice. The FTC has stated that a substantial injury often "involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction."[8] Emotional harm, and nothing more, likely will not constitute unfairness, according to the Commission.[9] In the cybersecurity world, this means that a company is more likely to face an FTC action if the Commission finds that a data breach led to actual consumer harm, such as identity theft. Absent such actual harm, the FTC is less likely to bring an action for a data breach.

Second, do benefits to consumers outweigh the injury?[10] The FTC states that it "will not find that a practice unfairly injures consumers unless it is injurious in its net effects."[11] The Commission states that it considers "the various costs that a remedy would entail," including:

- direct costs to the parties;
- paperwork;
- restrictions on information flows;
- reduced innovation; and
- restrictions on capital formation.

This means that if a company suffers a data breach that leads to substantial consumer injury, a company may be able to avoid an FTC action if the company can demonstrate that it would have been very difficult for the company to avoid the data breach. Note that this is a very high bar; a company cannot merely argue that cybersecurity safeguards were too expensive. The company must be able to demonstrate that either the remedy would have been impossible or the costs would have been so high that customers would have suffered even more than they did because of the data breach.

Third, the Commission considers whether consumers, exercising reasonable care, could have avoided the injury in the first place.[12] This prong reflects the FTC's market-based approach to consumer protection. The Commission states that it relies on "consumer choice – the ability of individual consumers to make their own private purchasing decisions without regulatory intervention."[13] The Commission becomes more likely to find a practice to be unfair if the consumer

8 FTC Unfairness Policy Statement.
9 *Id.*
10 *Id.*
11 *Id.*
12 *Id.*
13 *Id.*

was unable to reasonably avoid the harm.[14] Applying this to cybersecurity, the FTC is unlikely to take action against a company for a breach or other attack if customers could have taken simple steps to avoid harm. For instance, if a customer's failure to install updates on an operating system led to a virus that deleted all of the customer's files from the hard drive, the customer is not very likely to succeed in a lawsuit against the maker of the operating system. In contrast, a consumer might successfully sue a company whose internal servers were hacked, leading to disclosure of the customer's personal financial information and, subsequently, identity theft. In that circumstance, it is difficult to imagine how the customer would have reasonably avoided the harm.

The FTC has not issued binding regulations that explain how these three principles apply to cybersecurity. That has led a number of businesses and industry groups to criticize the agency for failing to provide concrete standards. After all, they argue, a company will be more hesitant to invest significant time, money, and resources in cybersecurity measures if it is not even sure whether these investments would satisfy the FTC's expectations. The FTC and its defenders, however, argue that cybersecurity is not a one-size-fits-all solution, and a company's safeguards should depend on its unique needs. For instance, a hospital likely stores vast amounts of highly confidential medical data; thus, it might be expected to take greater security precautions than a company that does not typically process or store personal information. Likewise, if a company has experienced a cybersecurity incident, it would be on notice of such vulnerabilities and expected to take reasonable steps to prevent future incidents.

1.1.2 Wyndham: Does the FTC have Authority to Regulate Data Security under Section 5 of the FTC Act?

An August 2015 opinion from the U.S. Court of Appeals for the Third Circuit – arising from a cybersecurity complaint that the FTC filed against the Wyndham hotel chain – is the most important court decision to date involving the Commission's cybersecurity authority. In short, the opinion provides the most compelling authority for the Commission to use Section 5 to bring cases against companies that have failed to adequately secure personal information.

Up to this point, the FTC's regulation of privacy and data security had been a source of frustration for many companies. As discussed above, Congress has not passed a statute that provides the FTC with the general authority to regulate

14 *Id.* ("[I]t has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.")

cybersecurity. Instead, the FTC claims that inadequate data security may constitute an unfair or deceptive trade practice under Section 5 of the FTC Act, which Congress initially passed more than a century ago.

Although many commentators have long challenged the FTC's cybersecurity authority, it typically has been widely accepted. In the vast majority of cases, if the FTC threatens to file a lawsuit against a company arising from allegedly inadequate cybersecurity, the company agrees to a consent order. Although the terms vary by company, the orders generally require companies to develop comprehensive information security programs, obtain periodic independent assessments of their information security, and provide the FTC with broad oversight and access into the company's programs for up to twenty years. Failure to adhere to the order can result in significant fines. Despite the potential for draconian penalties, companies generally do not risk the publicity and costs of challenging the FTC's findings in court, and instead agree to a consent order.

Wyndham Worldwide Corporation, a hotel chain, decided to become among the first companies to mount a serious challenge to the FTC's cybersecurity enforcement authority.[15] In 2008 and 2009, hackers stole hundreds of thousands of Wyndham customers' financial information and charged more than $10 million to consumer accounts.[16] After investigating the breaches, the FTC claimed that Wyndham failed to take numerous steps to safeguard customer information, leading to the compromises. Patent among the failures that the FTC cited were:

- storing credit card data in clear text;
- allowing simple passwords for the systems that store the sensitive data;
- failure to use firewalls and similarly standard cybersecurity technology;
- failure to adequately oversee the cybersecurity of hotels that connect to Wyndham's central servers;
- allowing vendors to have unnecessary access to Wyndham servers; and
- failure to take "reasonable measures" for security investigations or incident response.[17]

Altogether, the FTC alleged that these failures constituted unfair trade practices that violated Section 5 of the FTC Act. Rather than agree to a consent order, Wyndham allowed the FTC to file a lawsuit against the company in federal court. Wyndham moved to dismiss the lawsuit, arguing, among other things, that Section 5 does not provide the FTC with the authority to bring cybersecurity-related actions against companies.[18] The gravamen of Wyndham's argument was that Congress has addressed data security in industry-specific

15 FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
16 *Id*. at 240.
17 *Id*. at 240–41.
18 *Id*. at 242.

statutes for healthcare, banking, and credit reporting, and therefore, if Congress had intended to provide the FTC with the authority to regulate data security for all businesses, it would have explicitly granted the Commission such power. The district court disagreed and denied the motion to dismiss, holding that "the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme."[19] Soon after the ruling, the district court granted Wyndham's request for the U.S. Court of Appeals for the Third Circuit to review its ruling. This was particularly significant because, until that point, no federal appellate court had ever ruled whether the FTC has the authority to bring cybersecurity-related actions.

After hearing oral argument, the Third Circuit in March 2015 issued a 47-page opinion in which it upheld the District Court and ruled that the "unfairness" prong of Section 5 provides the Commission with the authority to regulate data security. Although the Court's ruling is only binding in the Third Circuit – Delaware, New Jersey, Pennsylvania, and the U.S. Virgin Islands – it was widely seen as an affirmation of the FTC's jurisdiction over cybersecurity.

Relying on dictionary definitions, Wyndham argued that "unfair" conditions only exist if they are "not equitable" or are "marked by injustice, partiality, or deception."[20] The Third Circuit declined to rule whether such deception is necessary to demonstrate unfairness; it concluded that a company "does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."[21]

Wyndham also argued that a business "does not treat its customers in an 'unfair' manner when the business *itself* is victimized by criminals."[22] The Third Circuit rejected this argument, concluding that the fact "that a company's conduct was not *the most* proximate cause of an injury does not immunize liability from foreseeable harms."[23] The Court noted that Wyndham did not argue that the breaches were unforeseeable, a stance that the Court believed "would be particularly implausible as to the second and third attacks."[24]

The Third Circuit also gave little weight to Wyndham's argument that allowing the lawsuit to proceed would effectively provide the FTC with unlimited authority under the unfairness prong. Wyndham argued that such a result would mean that the Commission could use Section 5 to "regulate the locks on hotel room doors, … to require every store in the land to post an armed guard at the door, and to sue supermarkets that are sloppy about sweeping up banana

19 FTC v. Wyndham Worldwide Corp., 10 F.Supp. 3d 602, 613 (D. N.J. 2014).
20 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245 (3d Cir. 2015).
21 *Id*.
22 *Id*. at 246.
23 *Id*.
24 *Id*.

peels."[25] The Court dismissed this argument as "alarmist," noting that "were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune" from a Section 5 action.[26]

Like the District Court, the Third Circuit disagreed with Wyndham's argument that Congress's passage of data security laws for banking, credit reporting, and other specific sectors demonstrates that the FTC does not have general authority over cybersecurity. The FTC noted that many of these laws focus on the *collection* of data, and do not conflict with regulation of the data *security*.[27]

In addition to arguing that the FTC lacked the statutory authority to bring general data security enforcement actions, Wyndham also asserted that the FTC's action violates the Due Process Clause of the U.S. Constitution because it failed "to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement."[28] As the Third Circuit accurately summarized, Wyndham's position is that "the FTC has not yet declared that cybersecurity practices can be unfair; there is no relevant FTC rule, adjudication or document that merits deference; and the FTC is asking the federal courts to interpret [Section 5 of the FTC Act] in the first instance to decide whether it prohibits the alleged conduct here."[29]

The Third Circuit concluded that Wyndham was only entitled to "fair notice that its conduct could fall within the meaning of the statute," and it was not entitled "to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required" by Section 5 of the FTC Act.[30] The Third Circuit concluded that Wyndham had such notice, as the Commission, for years, had filed complaints arising from similar data security practices.[31]

Rather than asking all the judges on the Third Circuit to review the opinion *en banc*, or request the United States Supreme Court to hear the case, in December 2015 Wyndham settled the charges with the FTC. Wyndham agreed to implement a companywide data security program, undergo extensive payment card security audits, and take other precautions.[32] The order is in place for twenty years, as is standard for FTC data security settlements.

Although the *Wyndham* case has settled – and likely will not reappear unless the Commission alleges that Wyndham has violated its consent order – the case's

---

25 *Id*. at 246–47.
26 *Id*. at 247.
27 *Id*. at 248.
28 *Id*. at 249, quoting FCC v. Fox Television Stations, Inc., ___ U.S. ___, 132 S. Ct. 2307, 2317 (2012).
29 *Id*. at 253.
30 *Id*. at 255.
31 *Id*. at 257–58.
32 Press Release, Federal Trade Commission, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk (Dec. 9, 2015).

impact cannot be understated. Even though the ruling is only binding in the Third Circuit, it is the only federal appellate court ruling to consider whether the FTC has general data security enforcement authority. The ruling was a significant boost to the FTC's position that Section 5 allows it to regulate cybersecurity.

The ruling also led critics to bolster their criticisms of the FTC. While there is little dispute that private sector cybersecurity needs government support *and* regulation, a number of critics question whether an agency tasked with antitrust and consumer protection is the best equipped to carry out that mission.[33] Unless the Supreme Court overrules the Third Circuit's ruling, it is likely that the FTC's role as the de facto regulator of private sector data security will become more entrenched.

1.1.3 LabMD: What Constitutes "Unfair" or "Deceptive" Data Security?

In the only other significant challenge to the FTC's cybersecurity enforcement authority, LabMD, a medical testing laboratory, convinced an FTC administrative law judge to rule that the Commission's lawyers had failed to demonstrate that the company's alleged inadequate data security safeguards had caused or was likely to cause substantial injury to the company's consumers. However, in July 2016, the full Federal Trade Commission reversed the judge's ruling, in a significant victory for data security regulators.

In the LabMD case, the FTC's Complaint focused on two data security incidents at the company. The first arose from a report by a third party that a LabMD insurance aging report containing personal information of more than 9000 patients had been made public on a peer-to-peer network in 2008.[34] In the second incident, in 2012, documents containing personal information including names and Social Security numbers were found in the possession of unauthorized individuals.[35]

The Commission alleged in its Complaint that these two security incidents were due to a number of failures to take adequate safeguards, including:

- developing an information security program;
- identifying risks;

---

33 *See, e.g.*, Paul Rosenweig, The FTC Takes Charge – FTC v. Wynham, Lawfare (Aug. 26, 2015). ("All of this means that the FTC now owns cybersecurity in the private sector. Which is an odd result. One would surely have thought that DHS (or DoD or DOJ or even the Department of Commerce) would have had a more salient role in defining standards for the private sector. But somehow, we've converted a consumer protection mandate into a cybersecurity obligation and assigned that role to an independent agency. Candidly, I don't think the FTC is up to the task – not in terms of staffing nor in terms of expertise – but we will soon see how that turns out.")

34 In the Matter of LabMD Inc., No. 9537 (FTC Administrative Law Judge Nov. 13, 2015) at 1–2.

35 *Id*. at 2.

- preventing LabMD employees from unnecessarily accessing personal information;
- training employees regarding information security;
- requiring common authentication security for remote access to LabMD's network;
- maintaining and updating LabMD operating systems; and
- employing "readily available" prevention and detection measures.[36]

The FTC Administrative Law Judge (ALJ) collected extensive evidence, and ultimately granted LabMD's motion to dismiss the complaint. The ALJ focused on Section 5(n)'s requirement that the trade practice cause or be likely to cause substantial injury to customers. The ALJ ruled that the section "is clear that finding of actual or likely substantial consumer injury, which is also not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition, is a legal precondition to finding a respondent liable for unfair conduct."[37] The ALJ concluded that the preponderance of the evidence did not show that LabMD's "alleged unreasonable data security caused, or is likely to cause, substantial consumer injury."[38]

The FTC lawyers argued that even though there was not *actual* harm of identity theft, Section 5(n) also allows actions arising from "likely" harm. The ALJ, however, concluded that the failure to produce any evidence of consumer harm, "even after the passage of many years," undermines this argument.[39] After reviewing extensive Section 5 case law, the ALJ concluded that there is no known case in which "unfair conduct liability has been imposed without proof of actual harm, on the basis of predicted 'likely' harm alone."[40]

The ALJ's LabMD ruling is so important to data security because it stands for the proposition that the mere threat of identity theft after a data breach is not sufficient grounds for a Section 5 claim. This ruling, if it had become binding law, could have made it significantly harder for the FTC to bring cases under Section 5.

Accordingly, consumer and privacy advocates were relieved on July 29, 2016, when the full Federal Trade Commission reversed the ALJ's dismissal of charges against LabMD. The Commission's unanimous ruling was not entirely surprising, as the Commissioners had long defended the Commission's authority to regulate data security under Section 5. In its opinion, the Commission wrote that a demonstration of a "significant risk" of injury is sufficient to meet Section 5's "likely to cause" requirement.[41] Exposing sensitive personal information to millions of people via peer-to-peer networking, the Commission

36 *Id*.
37 *Id*. at 48.
38 *Id*. at 49.
39 *Id*. at 52.
40 *Id*. at 53.
41 In the Matter of LabMD Inc., No. 9537 (Commission Opinion and Order, July 29, 2016) at 21.

reasoned, creates a significant risk of injury and therefore satisfies this requirement.[42]

As of the publication of this book, LabMD was expected by some commentators to appeal the FTC's ruling to the U.S. Court of Appeals for the Eleventh Circuit but had not yet done so.

1.1.4 FTC June 2015 Guidance on Data Security

In the face of criticism that it did not clearly articulate the standards to which it holds companies for data security, in June 2015, the FTC released a highly publicized document, *Start with Security: A Guide for Business*.[43] The guide was not formally approved by the Commission as a regulation, and therefore it is not binding in court, as regulations would be. Instead, the booklet draws on the facts of data security-related enforcement actions that the FTC has brought against companies, and provides ten over-arching principles to help guide companies as they develop their cybersecurity programs.

Even though the guide does not carry the force of law, it is noteworthy because the FTC rarely provides any guidance whatsoever regarding data security. Accordingly, it is important to consider the ten principles that the FTC articulated in the guide, and an analysis of how these principles might apply to businesses:

1) ***Start with security***. The Commission urges businesses to consider security in every aspect of their decision making. Businesses should not collect unnecessary information, and they should dispose of information after it has served its purpose. Companies also should avoid unnecessary use of personal information.
2) ***Control access to data sensibly.*** The Commission advises businesses to allow employees to access sensitive data, such as financial account numbers, only if those employees have a valid business reason to access that data. For example, a human resources manager may have a valid reason to have access to employees' payroll data. But an entry-level marketing employee probably does not have a valid reason to access the payroll records of all employees. The Commission also recommends that companies limit the number of employees who have administrative access to make changes to the entire system.
3) ***Require secure passwords and authentication.*** A common vulnerability that leads to data breaches and other incidents is the failure of organizations to require strong passwords. Indeed, a recent survey found that the five most common passwords in 2014 were 123456, password, 12345, 12345678, and

42 *Id.*

43 Federal Trade Commission, Start with Security: A Guide for Business (June 2015).

qwerty.[44] To compound problems, people often fail to change their passwords. Forty-seven percent of passwords in 2014 were at least five years old.[45] The FTC suggests that organizations require individuals to choose complex passwords. The Commission does not specify a minimum number of characters, but it suggests prohibiting passwords that are common dictionary words. The Commission also urges organizations to prevent employees from unnecessarily exposing passwords, such as by storing them in personal email accounts. Finally, the Commission notes that hackers often guess passwords through "brute force attacks" in which automatic programs guess combinations of characters until they hit the correct passwords. The Commission said that companies can reduce the threat of brute force attacks by limiting the number of attempted log-ins. Some risk-averse companies limit the number of failed log-in attempts to five or three. After that point, the account is locked, and the user must call an administrator to reactivate access.

4) ***Store sensitive personal information securely and protect it during transmission.*** The Commission appears to recognize that certain types of sensitive personal information, such as health records, require particularly strong security measures. Although the Commission does not provide a specific definition of "sensitive" information, it strongly encourages businesses to use strong cryptography – such as hashes and Transport Layer Security/Secure Sockets Layer – on any information that they deem to be sensitive. The Commission urges companies to use industry-standard security measures, and to avoid adopting encryption methods that have not been tested (though the Commission did not point to a specific industry standard). Sensitive data should be secured throughout its life cycle, both in transit and at rest on a company's server.
5) ***Segment your network and monitor who's trying to get in and out.*** The Commission suggests that companies segregate particularly sensitive data from other parts of the network. For instance, a retail company should segment the computers that store credit card information so that the card numbers are not accessible from every computer on the network. Furthermore, the Commission urges companies to monitor access logs to detect unusual activity.
6) ***Secure remote access to your network.*** Bring Your Own Device (BYOD) programs[46] and virtual private networks are increasingly popular options

---

44 Carly Okyle, *Password Statistics: The Bad, the Worse, and the Ugly*, Entrepreneur (June 3, 2015).

45 *Id*.

46 *See* Matt Straz, *Employees Feel the Love When Companies Embrace BYOD*, Entrepreneur (June 15, 2015). ("BYOD is when a business allows employees to use personal devices at work, ranging from smartphones to tablets to laptops, or devices sanctioned by the company and supported alongside devices that are business-owned.")

that enable employees to access corporate email and files on their own mobile devices. However, these devices present a number of serious cybersecurity challenges. The Commission urges businesses to ensure that these devices and computers contain adequate security measures. For instance, if an employee accesses a company's VPN via a personal computer that is infected with malware, a hacker could track all of that employee's keystrokes – including usernames and passwords. Accordingly, companies would be wise to require employees to have antivirus programs and firewalls on their computers. Companies also should require that mobile devices used for BYOD be secured with sufficiently complex passwords. It is increasingly common, for example, for companies to require employees to use device passcodes that are longer than many smartphones' default minimum of four characters.[47] For VPN access, it is increasingly common – and wise – for companies to require two-factor authentication (e.g., a password and a token).

7) ***Apply sound security practices when developing new products.*** The Commission has made it crystal clear that it will not allow companies to avoid responsibility for cybersecurity incidents by blaming engineers or other technical employees. Indeed, the FTC expects those who design products and services to have the same understanding of security practices as lawyers and managers. The FTC requires employees at all levels of the organization – including engineers – to prioritize cybersecurity. The Commission expects companies to provide all engineers with secure coding training, and it has brought actions against companies whose engineers did not employ industry-standard coding practices. Furthermore, if a platform such as IOS has default security settings, the Commission expects that app or software developers will not circumvent that security. The Commission also urges companies to test apps and software to ensure that the security measures function properly, and to regularly test software and apps for vulnerabilities.
8) ***Make sure your service providers implement reasonable security measures.*** Just as companies cannot avoid responsibility for breaches by blaming employees, they cannot shift the responsibility to service providers. The FTC warns that companies must "keep a watchful eye" on their service providers. In the age of subcontractors and sub-subcontractors, of course, this can be quite a difficult task. However, it is necessary, at minimum, to require adequate security in contractors with service providers, and to monitor their compliance with these standards. The FTC states that companies could reduce the risks of security vulnerabilities caused by subcontracts by "asking questions and following up with the service provider during the development process."

47 *See 13 Best Practices for Developing Your Mobile Device Policy*, NetStandard (Aug. 6, 2013).

9) ***Put procedures in place to keep your security current and address vulnerabilities that may arise.*** The Commission urges companies to keep in mind that cybersecurity "Isn't a one-and-done deal." If a software provider provides a patch, the FTC expects that a company will promptly install that patch. If companies receive "credible security warnings," the Commission says, they must quickly remediate those problems. For instance, independent security researchers often alert companies to vulnerabilities that they have detected. The FTC has made clear that companies cannot turn a blind eye to such warnings. The Commission suggests that companies establish a dedicated email address for security reports.
10) ***Secure paper, physical media, and devices.*** Cybersecurity involves both data *and* physical security. The Commission has brought actions against companies that have failed to secure papers that contain sensitive information. Moreover, the Commission expects companies to physically secure computers and devices that contain sensitive information. Likewise, the Commission has brought enforcement actions against companies whose data has been compromised because employees have lost laptops. If employees store sensitive information on laptops, it is wise to encrypt the laptops. Finally, the FTC expects that companies securely dispose of all data – whether in electronic or paper form.

1.1.5 FTC *Protecting Personal Information* Guide

In November 2011, the FTC released *Protecting Personal Information: A Guide for Businesses*. The 15-page guide is less specific about particular technologies than *Start with Security*. Also unlike the subsequent guidance, *Protecting Personal Information* does not cite specific FTC actions or complaints for its guidance. Instead, *Protecting Personal Information* provides a five-step framework that companies should consider when developing their cybersecurity plans:

1) ***Take stock.*** Businesses should conduct routine and comprehensive inventories of the personal information on all of their computers, servers, and other storage facilities. Businesses should know who can access the data, the types of data that businesses maintain, and where the data is stored.
2) ***Scale down.*** The Commission urges businesses to only retain personal information that is necessary for business operations and customer services. Moreover, a number of statutory restrictions limit the types of information that can be stored and distributed. For instance, Social Security numbers may not be used as general customer identifiers, and businesses are required to redact all but the last five digits of a payment card number from a receipt.
3) ***Lock it.*** To the extent that businesses have a legitimate need to retain personal information, they must take proper physical, administrative, and

technical safeguards to protect that information from unauthorized access and disclosure. The Commission is particularly focused on the need to employ technical measures such as firewalls and encryption to safeguard personal information. The Commission also urges businesses to restrict employee access to mobile storage – such as laptops. The FTC encourages businesses to regularly train employees regarding proper security practices, and to conduct thorough inquiries of the data security of potential service providers.

4) ***Pitch it.*** The Commission encourages businesses to securely destroy personal information once it is no longer necessary. For paper documents, the FTC encourages effective shredding. For computers and other electronic storage, companies must use software that fully deletes the data before discarding the equipment.
5) ***Plan ahead.*** The Commission encourages companies to develop detailed incident response plans that delegate roles and duties immediately after a data breach. In particular, companies should consider how to prevent further harm, as well as their obligations to notify individuals, regulators, law enforcement, and others.

1.1.6 Lessons from FTC Cybersecurity Complaints

With rare exceptions such as the *Wyndham* cases, the vast majority of FTC cybersecurity investigations do not result in court opinions or judgments. That is because most of these cases quietly settle, with the company agreeing to remediation measures and oversight by the FTC for up to twenty years.

The FTC's *Start with Security* guidance, described above, is perhaps the Commission's clearest statement about some factors that it considers when determining whether a cybersecurity measure (or lack thereof) constitutes "unfair" or "deceptive" trade practice. However, the document is relatively short and does not even purport to cover every possible cybersecurity safeguard and vulnerability.

The complaints that the FTC has filed against companies provide the most useful guidance as to what types of cybersecurity safeguards (or lack thereof) are most likely to result in the FTC investigating a company and filing an enforcement action. (Indeed, the FTC's guidance is based on its positions in these cases.) Below is a more complete summary of the cybersecurity-related complaints that the FTC has filed in the past decade, with a focus on the incidents that the FTC alleges to constitute a violation of Section 5. Keep in mind that all of these complaints resulted in a settlement agreement before the FTC even had the opportunity to file a lawsuit in court, so there is a chance that a court would disagree with the FTC and conclude that the company had implemented adequate data security safeguards. By settling with the FTC, the companies did not admit any wrongdoing.

Although all of the complaints involve Section 5 allegations, I have categorized them into three general types of complaints: (1) security of highly

sensitive personal information, (2) security of payment card information, and (3) security violations that contradict privacy policies. The FTC also has brought a number of complaints that allege inadequate cybersecurity practices by financial institutions, in violation of the Gramm–Leach–Bliley Act; those cases are discussed in Chapter 9.

The FTC also brings Section 5 cases against companies that it believes violated customer privacy. For instance, if a company promises to keep customer personal information confidential, and proceeds to sell that data to third parties, the FTC may bring a Section 5 complaint against that company. Because the focus of this section is *security*, I have not included purely privacy-focused Section 5 cases. However, I included cases that include both privacy- *and* security-related claims.

When possible, the docket numbers for the FTC cases are included below. To obtain the full case information, including FTC complaints, press releases, and consent decrees, visit www.ftc.gov and enter the docket number.

1.1.6.1 Failure to Secure Highly Sensitive Information

Unlike other jurisdictions, such as the European Union, the FTC does not have a formal definition of "sensitive" information. However, the FTC is more likely to bring a complaint against a company if it has failed to safeguard particularly sensitive forms of information. As the cases below demonstrate, the FTC considers data to be particularly "sensitive" if it reveals a health condition or other highly personal trait, or if its unauthorized disclosure is likely to lead to identity theft (e.g., a Social Security number or full credit card number).

The FTC general expects companies to adopt industry-standard practices for sensitive data. Among these practices are strong encryption, securing both electronic *and* physical access, routine audits, penetration testing, and other common safeguards.

1.1.6.1.1 Use Industry-Standard Encryption for Sensitive Data

***In the Matter of Henry Schein Practice Solutions, Inc.*, Docket No. C-4575 (2016)** Henry Schein Practice Solutions makes software that dentists use to enter and store patient medical records. The company used a database engine provided by an outside vendor. The engine protected the data with a proprietary algorithm that the vendor told Henry Schein was less secure than industry-standard encryption algorithms that are recommended by the Department of Health and Human Services and the National Institute of Standards and Technology. Nonetheless, Henry Schein promoted its software as offering "new encryption capabilities that can help keep patient records safe and secure." In 2013, the U.S. Computer Emergency Readiness Team issued an alert about the company's software as containing a "weak obfuscation algorithm," yet for several months after that alert, the company continued to market the claim that it "encrypts" patient data. The FTC brought a complaint against Henry Schein,

alleging that despite its representations, the software "used technology that was less secure than industry-standard encryption."

Key Lesson Although NIST and the U.S. Computer Emergency Readiness Team do not regulate agencies, they are among the leading voices on encryption and data protection. Accordingly, if either of those agencies specifically criticizes a company's data security technology, there is a good chance that an FTC complaint will soon follow.

1.1.6.1.2 Routine Audits and Penetration Testing are Expected

***In the Matter of Reed Elsevier Inc. and Seisint Inc.,* No. C-4226 (2008)** Reed Elsevier operates LexisNexis, which provides companies with databases of information about individuals. Companies that used these verification services include landlords, debt collectors, and potential employers. Among the data in the company's databases were individuals' credit reports, driving records, and Social Security numbers. Recognizing the sensitivity of the information, the company imposed a number of safeguards, including authentication of customers who accessed the databases, formatting requirements for the credentials that customers use to authenticate, and restrictions on access to nonpublic personal information. These safeguards, however, were not strong enough to prevent a breach of these databases. Unauthorized users obtained a customer's user ID and password and accessed the sensitive information – including names, addresses, birth dates, and Social Security numbers – of more than 300,000 individuals. In some cases, the thieves used this information to open credit accounts in the individuals' names. The FTC filed a complaint against the company, alleging that the breach was caused, in part, by the company's failure to take the following precautions:

- Prohibiting customers from using common dictionary words as their passwords and user IDs;
- Allowing LexisNexis customer to share credentials with others;
- Failing to require users to change their passwords routinely (the FTC used every 90 days as an example);
- Failing to limit the number of unsuccessful attempts to log-in before suspending access;
- Allowing customers to log into Lexis-Nexis automatically by storing their credentials in cookies;
- Not requiring encryption of credentials or searches in transit;
- Failing to confirm a customer's identity before allowing the customer to create new credentials;
- Failing to assess the company website's vulnerability to certain common forms of attacks;

Key Lesson Companies cannot assume that data is secure merely because data is password protected. Companies must regularly assess the strength of their

authentication procedures and ensure that bad actors cannot bypass the authentication safeguards.

1.1.6.1.3 Health-Related Data Requires Especially Strong Safeguards

***In the Matter of Eli Lilly and Company,* No. 012 3214 (2002)** Eli Lilly, which manufactures the psychiatric drug Prozac, offered an email service, "Medi-Messenger," which provided customers with personal reminders regarding their medications. For instance, if a customer was due for a thirty-day refill of Prozac, the Medi-Messenger site, via Prozac.com, would email a reminder to the customer. As one might imagine, the mere fact that an individual has been prescribed an antidepressant is viewed as highly sensitive information.

About three months after launching Medi-Messenger, Eli Lilly decided to terminate the service. The company informed customers via a blast email. However, the email addresses of all 669 Medi-Messenger customers were visible in the "To" line of the email (rather than in the "BCC" line). This resulted in every recipient of the email being able to see the email addresses of the 668 other Eli Lilly customers who had registered for the Prozac medication reminder service.

The FTC alleged that Eli Lilly violated Section 5 by failing to adequately train and oversee the employee who sent out this particularly sensitive email. The Commission also argued that Eli Lilly should have reviewed the email before sending and tested the email system to ensure that such a communication would not reveal the email addresses of the customers.

This complaint – one of the FTC earliest data security-related enforcement actions – is instructive on two fronts. First, it demonstrates that the FTC will hold a company accountable for the actions of one employee, no matter how inept or negligent. The employer ultimately is responsible for ensuring that *every* employee safeguards customer data. Second, the complaint illustrates that the FTC does not treat all types of data the same; it considers the sensitivity. The FTC's concern was not merely that email addresses were exposed; the truly egregious violation occurred because those email addresses were associated with the fact that the individuals had been prescribed psychiatric medications. Had the program instead been a weekly reminder for customers to go grocery shopping or pay their water bills, it is unclear whether the FTC would have shown a similar level of concern.

Key Lesson Companies that handle particularly sensitive information should carefully oversee the employees who handle that information, and provide regular, comprehensive cybersecurity training. Although healthcare-related data also is subject to requirements under the Health Information Portability and Accountability Act (HIPAA), disclosure of particularly sensitive information also could give rise to a Section 5 complaint from the FTC.

In the Matter of CBR Systems, Inc., Docket No. C-4400 (2013) CBR collects umbilical cord blood during the delivery of babies, and banks it for potential future medical use. When processing orders from potential clients, CBR collects personal information including the names, addresses, Social Security numbers, credit card numbers, blood types, medical histories, and adoption histories of families. Information about nearly 300,000 individuals was backed up on four unencrypted tapes, which a CBR employee placed in a backpack to transport between two CBR facilities in California. The employee left the backup tapes, along with a CBR laptop and hard drive, in a personal vehicle that was broken into overnight. The laptop and hard drive contained unencrypted information that could enable an unauthorized user to access other personal information on the company's network.

The FTC brought a complaint against CBR, alleging that it violated the FTC Act by allowing its employee to transport unencrypted personal information in a backpack, and failing 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."

Key Lesson This case demonstrates that the FTC expects companies to take exceptional care when handling information such as medical histories and adoption records. The Commission also expects companies to ensure that they safeguard not only the personal information stored on their networks but also the credentials and other tools that could be used to access that information.

1.1.6.1.4 Data Security Protection Extends to Paper Documents

In the Matter of CVS Caremark Corporation, C-2459 (2009) CVS, one of the largest pharmacy chains in the United States, improperly disposed of papers containing customers' personal information in pharmacies in fifteen cities. Among the records were pharmacy labels, credit card receipts, and prescription purchase refunds. Journalists reported that CVS had disposed of these records in public dumpsters. The FTC alleged that CVS failed to implement "reasonable and appropriate measures to protect personal information against unauthorized access," and violated its own privacy policy, which stated that "nothing is more central to our operations than maintaining the privacy of your health information."

Key Lesson Discussions about "data security" typically involve information that is stored on computers. Indeed, although FTC data security enforcement typically focuses on computer data, the Commission also will bring actions against companies that fail to properly safeguard data in physical form, such as paper records and credit card receipts. Likewise, physically disposing of a computer could raise concerns with the FTC if the company has not taken proper steps

to ensure that all personal information has been permanently removed from the computer before disposal.

***PLS Financial Services*, Case 1:12-cv-08334 (E.D. Ill.)** Similarly, the FTC filed a complaint in the federal court against PLS, which operated payday loan retailers in Illinois. The FTC accused the company of disposing of boxes of consumer records that included a great deal of sensitive information, including bank account numbers, wage data, applications for loans, and consumer reports. The FTC alleged that the company "failed to implement policies and procedures in key areas, including the physical security of sensitive consumer information; the proper collection, handling, and disposal of sensitive consumer information; and employee training regarding such matters."

Key Lesson The Commission's complaint focused on the failure of PLS to develop *written* policies regarding both electronic *and* physical data security. Accordingly, it is in a company's best interests to develop such policies, and to train employees to follow them. Too often, data security policies focus on electronic data and do not account for the possibility that physical records can contain highly sensitive data.

***In the Matter of Rite Aid Corporation*, Docket No. C-4308 (2010)** Television stations reported that Rite Aid, a large nationwide operator of retail pharmacies, had disposed of pharmacy labels, employment applications, and other documents containing sensitive information, in unsecured dumpsters. The FTC alleged that this data "could be misused to commit identity theft or to steal prescription medicines." The FTC attributed this incident to Rite Aid's failure to:

- implement secure disposal policies and procedures that would ensure that sensitive information is no longer readable;
- train employees on proper disposal methods;
- evaluate its data disposal procedures; and
- establish a "reasonable process" to mitigate disposal-related risks.

Key Lesson As with the CVS case, this case demonstrates that companies need not only care about the data that they store in their files and on servers but the data that they dispose of once it is no longer necessary for business purposes. Companies must not only discard the data, but they must ensure that it is no longer readable or capable of being reconstructed by a bad actor.

1.1.6.1.5 Business-to-Business Providers also are Accountable to the FTC For Security of Sensitive Data

***In the Matter of Ceridian Corporation*, Docket No. C-4325 (2011)** Ceridian provides online payroll processing services for small businesses that do not have internal payroll departments. To process employee payroll, the company must collect

employees' personal information, including addresses, Social Security numbers, birth dates, and bank account numbers. The company's website promised employers that its "comprehensive security program is designed in accordance with ISO 27000 series standards, industry best practices and federal, state and local regulatory requirements." Despite these promises, hackers used an SQL injection attack – a common hacking tool – to access the personal information of more than 27,000 individuals whose employers used Ceridian. The FTC determined that Ceridian had failed to take a number of reasonable security steps. Among the alleged failures: storing the information in clear text, storing the information indefinitely, neglecting to test its applications and networks for SQL injection attacks, and failing to employ standard detection and prevention measures.

Key Lesson Unlike retailers and other companies that collect personal information directly from consumers, Ceridian receives the information from a third party. Nonetheless, the FTC will hold service providers responsible for the security of personal information that they receive from business customers.

***In the Matter of Lookout Services*, C-4326 (2011)** Just as Ceridian is an outsourced payroll provider, Lookout Services outsources the employee citizenship verification required under federal law. To perform this service, Lookout collected a great deal of sensitive information, including employee Social Security numbers and passport numbers. Lookout's advertisements to potential customers stated that this data is transmitted securely and its interface "will protect your data from interception, as well as keep the data secure from unauthorized access." Lookout's website stated that its servers "are continuously monitoring attempted network attacks on a 24 × 7 basis, using sophisticated software tools."

Despite these alleged precautions, Lookout allegedly failed to implement a number of common security safeguards, including complex passwords, required password changes, and monitoring for unauthorized access. Users also were able to circumvent Lookout's authentication procedures altogether by typing a Lookout URL directly into their web browser. Such "backdoor access" is an easily preventable vulnerability. A Lookout user took advantage of this weakness and obtained more than 37,000 individuals' sensitive personal information. Two months later, the user guessed common passwords, such as "test," to again access the sensitive information.

Key Lesson Even if a company has implemented significant technical data security safeguards, its failure to implement adequate authentication policies may leave it vulnerable to scrutiny by the FTC. All companies – and particularly those that store and process particularly sensitive information – should ensure that their authentication procedures are industry standard, and that only properly authenticated users have access to the data.

***In the Matter of Accretive Health, Inc.,* Docket No. C-4432 (2014)** Accretive Health provides hospitals with a variety of administrative services, including bill collection, registration services, and transcription. Its employees work on-site at hospitals. In 2011, a laptop containing highly sensitive personal information about more than 23,000 patients of an Accretive client was stolen from an Accretive employee's car. The FTC complaint against Accretive alleged that the company did not take adequate steps to prevent employees from transporting personal information in an unsecure manner, and that Accretive had a duty to limit employee access to personal data only if the employees had a business need to access the information.

Key Lesson Even though the personal information belonged to customers of Accretive's clients – and not to Accretive's direct clients – the FTC nonetheless held Accretive fully responsible for the failure to safeguard the information.

1.1.6.1.6 Companies are Responsible for the Data Security Practices of Their Contractors

***In the Matter of GMR Transcription Services, Inc.,* Docket No. C-4482 (2014)** GMR Transcription services transcribes audio recordings for a variety of clients, including doctors and medical institutions. GMR customers typically upload audio files via GMR's website. GMR typists transcribe the audio into a Word document, and provide the transcript to the customer either via email or GMR's computer network. The FTC alleges that Fedtrans, an India-based contractor for GMR, stored audio files and transcripts on an unsecure FTP application that was accessible to unauthenticated users. Indeed, the FTC was able to find thousands of GMR transcripts via a major search engine. These files contained particularly sensitive information, including names, medications, employment history, and medical records. The FTC complaint alleged that GMR caused this exposure by failing to require that its contractors adhere to standard data security safeguards, such as requiring Fedtrans and other service providers, in the service contracts, to implement "reasonable and appropriate security measures to protect personal information in audio and transcript files" that are stored on the contractors' networks. For instance, the FTC cited GMR's failure to require contractors to encrypt storage and transmission of audio and transcript files, and to require strong authentication measures before typists could access the data. The FTC also asserted that GMR failed to adequately oversee the contractor's data security practices through audits or requests for written security policies and procedures.

Key Lesson Just as the FTC holds service providers responsible for how they handle the personal information of their clients' customers, the FTC also will hold companies accountable for the data security practices of their service providers. Accordingly, it is a best practice to contractually require service providers to adopt industry-standard data security measures, particularly for sensitive information. Moreover, the FTC believes that companies have a duty

to regularly oversee the data security practices of their contractors, through audits and other routine reviews.

1.1.6.1.7 Make Sure that Every *Employee Receives Regular Data Security Training for Processing Sensitive Data*

***In the Matter of Franklin's Budget Car Sales, Inc., also dba Franklin Toyota Scion,* C-4371 (2012)** Personal information of about 95,000 customers of Franklin's Budget Car Sales, a car dealership, was made available on a peer-to-peer network that a Franklin's employee had installed on his work computer. Among the information allegedly disclosed were drivers' license numbers and Social Security numbers. Peer-to-peer networks are not only the source of a great deal of intellectual property infringement (through sharing videos and music) and illegal content (e.g., child pornography), they also carry viruses and other malware that exposes a computer – and the network to which it was connected – to data theft. After an investigation, the FTC criticized Franklins for failing to implement a number of safeguards, including employee data security training, network monitoring, and promulgation of information security policies.

Key Lesson Employee behavior remains one of the most significant data security vulnerabilities for businesses. To avoid regulatory action after data breaches, employers must provide ongoing employee training, and reasonably monitor employees' use of information technology to ensure that the employees are not taking large risks, particularly if the employer's computers contain sensitive consumer information.

1.1.6.1.8 Privacy Matters, Even in Data Security

***In the Matter of Compete, Inc.,* No. C-4384 (2013)** Compete, a marketing company, provided customers with a free web browser tool bar, which provided them with information about the sites that they were surfing. It also offered a "Consumer Input Panel," which provided customers with the opportunity to win prizes in exchange for their product reviews. Compete's privacy policy stated that if a customer opted in, the company would only collect anonymous data about their web-browsing habits. The FTC alleged that this was untrue, and that the company, in fact, collected information about customers' online shopping, credit card numbers, web searches, and Social Security numbers. Although at first glance, this appears to be a privacy issue, it also involved data security because the FTC alleged that Compete failed to adequately safeguard this data, including by sending full bank account information in clear text. The FTC alleged that Compete's failure to adequately safeguard data created "unnecessary risk to consumers' personal information."

Key Lesson The FTC will take a particularly close look at a potential data security violation if the company had collected that data without obtaining the proper permission from consumers. Although such an act could be the basis

for a separate privacy-based claim, it could increase the chances that any subsequent data breach will receive extra regulatory scrutiny.

1.1.6.1.9 Limit the Sensitive Information Provided to Third Parties

***In the Matter of GeneLink, Inc.,* Docket Nos. C-4456 and 4457 (2014)** GeneLink provides cheek-swab kits to consumers, which collects their DNA information. After analyzing the DNA, GeneLink sells skincare products and nutritional supplements based on what the company determines to be their genetic needs. The FTC filed a lengthy complaint against GeneLink, largely focusing on the company's claims in its advertising and marketing. However, the complaint also included claims arising from inadequate data security. GeneLink's privacy policy stated that it provides some personal information to third-party subcontractors and agents, which "do not have the right to use the Personal Customer Information beyond what is necessary to assist or fulfill your order" and are "contractually obligated to maintain the confidentiality and security of the Personal Customer Information[.]" The FTC claimed that GeneLink took a number of "unnecessary risks" with customers' personal information, including providing all customer information to service providers, regardless of whether the providers needed that data.

Key Lesson Even if a company reserves the right to provide third parties with access to personal information, the FTC may closely scrutinize whether the company is unnecessarily putting customers' personal information at risk of unauthorized disclosure.

1.1.6.2 Failure to Secure Payment Card Information

As with particularly "sensitive" information such as health records and Social Security information, the FTC pays close attention to any breaches or exposures that involve payment card information, such as full credit card numbers, expiration dates, and security codes. It is important to note that companies that process or store payment card information also must comply with the Payment Card Industry Data Security Standard (PCI DSS), an industry-run program discussed in Chapter 3 of this book. However, in addition to the PCI DSS obligations, companies risk enforcement actions from the FTC if they do not properly handle payment card data.

1.1.6.2.1 Adhere to Security Claims about Payment Card Data

***In the Matter of Guess?, Inc.,* Docket No. C-4091 (2003)** This case, one of the FTC's earliest data security actions, arose when a hacker used an SQL injection attack on the clothing producer's ecommerce website to access customer credit card numbers. The Commission alleged that Guess? failed to adequately secure the data, by storing it in clear, unencrypted, and readable text. This was contrary to the company's privacy policy, which stated that Guess? uses SSL technology, which "encrypts files allowing only Guess? to decode your information." The FTC

alleged that the company failed to "detect reasonably foreseeable vulnerabilities of their website and application" and "prevent visitors to the website from exploiting such vulnerabilities and gaining access to sensitive consumer data," and therefore the claims in its privacy policy were misleading.

Key Lesson Any claims about security of payment card information must be strictly followed. If a breach later occurs, the FTC will closely scrutinize whether a company lived up to its claims about data security.

***In the Matter of Guidance Software, Inc.,* Docket No. C-4187 (2007)** Guidance Software provides business customers with a variety of information technology software and services, often focused on data security and breaches. As would be expected from a company in the cybersecurity field, Guidance issued a privacy policy that promised users that their sensitive information is protected, and that "information is encrypted and is protected with the best encryption software in the industry – SSL." The privacy policy also claimed that the company also does "everything in our power to protect user-information off-line" and "is committed to keeping the data you provide us secure and will take reasonable precautions to protect your information from loss, misuse, or alteration." A hacker used an SQL injection attack to obtain thousands of customer credit card numbers, security codes, and expiration dates, along with other personal information. In its complaint, the FTC noted that although Guidance did, in fact, use SSL encryption during transit, it allegedly stored the payment card data in clear text. The FTC also claimed that Guidance failed to adopt standard security measures and safeguards, nor did it regularly monitor outside connections to its network. The Commission asserted that the company failed to "detect reasonably foreseeable web application vulnerabilities" and "prevent attackers from exploiting such vulnerabilities and obtaining unauthorized access to sensitive personal information."

Key Lesson Companies that actively promote their cybersecurity safeguards – such as companies that sell security software and services – should be especially careful about the promises and guarantees that they provide to the public regarding payment card data.

1.1.6.2.2 Always Encrypt Payment Card Data

***In the Matter of Genica Corporation and Compgeeks.com and Geeks.com*, Docket No. C-4252 (2009)** Genica Corporation and its subsidiary, Compgeeks.com, operated a website, geeks.com, that sold computers and accessories. Its privacy policy stated that it uses "secure technology, privacy protection controls and restrictions on employee access in order to safeguard your personal information" and that it uses "state of the art technology (e.g., Secure Socket Layer, or SSL) encryption to keep customer personal information as secure as

possible." In fact, the website allegedly did not encrypt data, and instead stored payment card data and other personal customer information in clear text. During the first half of 2007, hackers repeatedly launched SQL injection attacks on the website and obtained hundreds of customers' payment card data.

Key Lesson Companies that collect and store credit card information should always encrypt the data, particularly if they promise security in their privacy policies.

1.1.6.2.3 Payment Card Data Should be Encrypted Both in Storage and at Rest

***In the Matter of Petco Animal Supplies, Inc.* (2004)** Petco, a large pet supply retailer, operates Petco.com, which sells products directly to consumers. The website's privacy policy assured customers that entering their credit card numbers "is completely safe," and that Petco.com's server "encrypts all of your information; no one except you can access it." In 2003, a hacker used an SQL injection attack to obtain complete credit card information from Petco.com's database. After investigating, the FTC determined that although the credit card data was encrypted in transit between the consumer's computer and Petco.com's server, Petco.com stored the data in unencrypted, clear text. The Commission, in its complaint, alleged that Petco "did not implement reasonable and appropriate measures to protect personal information it obtained from consumers through www.PETCO.com against unauthorized access."

Key Lesson Although encrypting payment card information while it is transit is a good first step, it is not sufficient to satisfy the FTC's standards. Payment card information also must be encrypted while it is stored on servers; otherwise, it could be vulnerable to relatively simple hacking.

***In the Matter of Life is good Retail, Inc.*, Docket No. C-4218 (2008)** Life is good, an online apparel retailer, promised customers in its privacy policy that "[a]ll information is kept in a secure file and is used to tailor our communications with you." In 2006, a hacker used an SQL injection attack on the company's website to access thousands of payment card numbers, security codes, and expiration dates. The FTC attributed this breach to the company's storage of payment card information in clear text, and its storage of the payment card information for an indefinite period of time. The Commission also alleged that the company failed to implement standard safeguards for payment card information, such as monitoring mechanisms and defensive measures.

Key Lesson Particularly if payment card data will be stored for a long period of time, the FTC likely will expect it to be encrypted while in storage.

1.1.6.2.4 In-Store Purchases Pose Significant Cybersecurity Risks

***In the Matter of BJ's Wholesale Club, Inc.*, Docket No. C-4148 (2005)** At the time of the FTC Complaint, BJ's operated 150 warehouse wholesale stores in the United States. The retailer accepted credit cards, and used its computers to

receive authorization from the issuing banks for the card purchases. BJ's usually transmitted the credit card data, obtained from the magnetic stripes on the cards, to a central BJ's data center, and then would send the information from there to the banks. BJ's also used wireless scanners, connected to its store computer networks, to collect information about its store inventory. In 2003 and 2004, BJ's customers' credit cards were used for numerous fraudulent purposes, causing thousands of customers to cancel and replace their credit and debit cards. The FTC alleged that BJ's inadequate security practices caused the fraudulent purposes. In particular, the FTC claimed that BJ's payment card security was inadequate because it failed to:

- encrypt payment card information both in transit and at rest;
- implement authorization safeguards that prohibit anonymous access to the data;
- restrict access to the in-store wireless networks;
- implement industry-standard intrusion detection programs; and
- delete the information after there is no business need (BJ's had been storing the data for 30 days, regardless of business need).

Key Lesson Retailers must take care to ensure that security of payment card data collected in stores is secure from unauthorized access. Particularly when a company operates hundreds of locations nationwide with thousands of employees, it may be difficult to control how each of those employees protects customer payment card data. However, it is clear that the FTC will hold companies accountable for in-store cybersecurity shortfalls.

***In the Matter of DSW Inc.,* Docket No. C-4157 (2006)** DSW, a footwear retailer that operated nearly 200 stores nationwide, suffered a data breach. In March 2005, DSW issued a press release announcing that credit card and purchase data was compromised. The next month, DSW announced in a second press release that checking account numbers, along with driver's license information, was compromised. In total, according to the FTC, the information for more than 1.4 million payment cards and 96,000 checking accounts was compromised, resulting in fraudulent charges on some of those accounts. The FTC asserted in its complaint that the breach was caused by DSW's failure "to provide reasonable and appropriate security for personal information collected at its stores." The data security shortfalls that the FTC identified include:

- storing payment card data in multiple files even though there was not a legitimate need to continue to retain the data;
- failing to secure its in-store wireless networks;
- failing to encrypt payment card information while it was in storage;
- allowing DSW in-store computers to connect to computers in other DSW stores and the corporate network, without adequate limits; and
- installing and implementing sufficient intrusion detection systems.

Key Lesson The DSW case illustrates the difficulty that many companies face when communicating with the public after a data breach or other security incident. Ideally, DSW would have only issued one press release that described all categories of data that had been compromised. However, such announcements involve a difficult balancing act: although data breach announcements should be thorough and complete, companies face pressure to inform the public of a data breach as quickly as possible to stem further damage.

***In the Matter of The TJX Companies, Inc.,* Docket No. C-4227 (2008)** In 2007, nationwide retailer The TJX Companies announced what at that time was believed to be the largest data breach in U.S. history. The company, which operates TJ Maxx and Marshalls retail chains, suffered a massive breach in which a hacker downloaded the payment card information of hundreds of thousands of customers between July 2005 and December 2006. The hacker accessed much of this data via Internet connections to TJX computers, where it was stored in clear text. Additionally, the hacker obtained some of the data while it was in transit between stores and TJX's central network. In total, TJX reports more than 45 million payment card numbers worldwide were stolen, though banks that later sued TJX argued that the number was closer to 100 million. In the year following the breach, TJX reported spending $250 million on the incident. The FTC filed a complaint against TJX, alleging that the breach was due to numerous cybersecurity shortcomings, including a failure to encrypt personal information while in transit and at rest, and a lack of "readily available security measures" for wireless access to its in-store networks. The Commission also noted that TJX failed to require strong passwords for authentication to its network, and did not use a firewall to isolate computers that stored payment card information.

Key Lesson The TJX data breach was enormous for its time, and led to some of the largest private sector cybersecurity lawsuits from customers and issuing banks (discussed in more detail later in Chapter 2). However, companies should keep in mind that besides private contract and tort litigation, they still could face an additional investigation and enforcement action from the FTC. In other words, private litigation and FTC actions are not mutually exclusive.

1.1.6.2.5 Minimize Duration of Storage of Payment Card Data

***In the Matter of CardSystems Solutions, Inc.,* Docket No. C-4168 (2006)** CardSystems Solutions provides credit card authentication services for retailers, and in 2005 processed at least $15 billion in purchases. In short, CardSystems acts as an intermediary between the retailer and the issuing bank, and communicates whether the purchase is approved or denied. A hacker used an SQL injection attack on CardSystems' website to obtain tens of millions of payment card numbers that the company had processed. The FTC alleges that this hack led to "several million dollars in fraudulent credit and debit card purchases that

had been made with counterfeit cards." The Commission, in its complaint, stated that CardSystems "created unnecessary risks to the information by storing it in a vulnerable format for up to 30 days." Additionally, the FTC alleged that CardSystems failed to assess whether its website was vulnerable to SQL injection attacks, failed to require employees to authenticate access with strong passwords, and neglected to implement a number of standard security and intrusion detection procedures and technologies.

Key Lesson Companies should *immediately* dispose of payment card data once it is no longer necessary for business purposes. CardSystems' blanket policy for retaining all payment card data for 30 days was clearly below the FTC's standards, particularly because the information was not encrypted.

1.1.6.2.6 Monitor Systems and Networks for Unauthorized Software

***In the Matter of Dave & Busters, Inc.,* Docket No. C-4291 (2010)** Dave & Busters, which operates more than 50 indoor entertainment centers nationwide, experienced a breach of about 130,000 customer payment card numbers. Hackers obtained this information by installing unauthorized software on the company's networks, allowing them to obtain the payment card data while it traveled from the stores to the company's credit card processing service provider. In its complaint against Dave & Busters, the FTC alleged that the company failed to adequately detect unauthorized access to its network and to monitor the third-party access to its network.

Key Lesson As with many data breaches, the hackers in the Dave & Busters case relied on software that they installed on the network to export the payment card data. Companies should routinely audit their systems to ensure that unauthorized software has not been installed by a third party.

1.1.6.2.7 Apps Should Never Override Default App Store Security Settings

***In the Matter of Fandango, LLC,* Docket No. C-4481 (2014)** Fandango provides an app for smartphones that allows customers to search for movie listing information and purchase tickets with their credit cards. When a customer purchases a ticket, the customer's app transmits the customer's complete payment card information to Fandango's servers. Fandango's privacy policy informs customers that when they purchase tickets via the iPhone app, the "information is securely stored on your device and transferred with your approval during each transaction." Apple, which provides the iOS system for the iPhone, uses application programming interfaces (APIs) that enable secure SSL connections, which provide encrypted communications. SSL communications use SSL certificates for both authentication and encryption. This prevents hackers from acting as middlemen and intercepting payment card data, a significant risk when customers use Wi-Fi connections at coffee shops, libraries, and other public locations. The default setting for iOS requires apps to use SSL certificates.

Apple warned developers that if they disable this default SSL setting, they will eliminate "any benefit you might otherwise have gotten from using a secure connection. The resulting connection is no safer than sending the request via unencrypted HTTP because it provides no protection from spoofing by a fake server." The FTC alleges that Fandango overrode this default setting and did not use the iOS SSL certificates. Fandango also failed to do any security testing that would have revealed that it was not using SSL. The FTC claimed that due to this failure, "attackers could have, in connection with attacks that redirect and intercept network traffic, decrypted, monitored, or altered any of the information transmitted from or to the application, including the consumer's credit card number, security code, expiration date, billing code, email address, and password."

Key Lesson As companies increasingly accept payment card information via apps, they should ensure that they accept all of the default app store security settings, unless they have a valid reason to do otherwise.

1.1.6.3 Failure to Adhere to Security Claims

Although the FTC pays particular attention to data breaches that compromise the security of sensitive information and payment card data, it is important to keep in mind that compromises of less sensitive information also could be on the FTC's radar. This is particularly true if the company's privacy policy, advertising, or other publicly available statement claims to provide specific data security protections, and the company nonetheless falls short. In other words, the FTC expects companies to adhere to their claims about cybersecurity, and it will pursue companies that it believes have broken their promises.

Even if a company's privacy policy or marketing materials do not explicitly guarantee a specific data security safeguard, the FTC may read broad statements about security and privacy to implicitly guarantee certain precautions. For instance, if a company's marketing materials guarantee customers that "we take every step to ensure the security of your information," and the company does not deactivate employees' log-in credentials after they leave the company, the FTC could reasonably conclude that the company's promise of security was misleading.

1.1.6.3.1 Companies Must Address Commonly Known Security Vulnerabilities

***In the Matter of MTS, Inc., d/b/a/ Tower Records/Books/Video and Tower Direct, LLC, Towerrecords.com*, Docket No. C-4110 (2004)** The companies operated TowerRecords.com, which sold music, videos, and other products via the Internet. The website's privacy policy claimed to "use state-of-the-art technology to safeguard your personal information." The policy also promised that the site "takes steps to ensure that your information is treated securely and in accordance with the relevant Terms of Service and this Privacy Policy." The FTC states that in 2002, when the website operator redesigned the site's

check-out functions, they created a vulnerability to enable any customer who entered an order number to view "the consumer's name, billing and shipping addresses, email address, phone number, whether the product purchased was a gift, and all Tower products purchased online." The FTC alleges that more than 5000 consumers' purchase information was accessed, and Internet chat rooms contained discussions about this security loophole. The FTC attributes this vulnerability to the companies' failure to "implement appropriate checks and controls on the process of writing and revising Web applications, adopt and implement policies and procedures regarding security tests for its Web applications, and provide appropriate training and oversight for their employees regarding Web application vulnerabilities and security testing." The FTC stated that such "broken account and session management" security risks had been "widely known" in the technology industry for years, and therefore, the companies misled consumers when they did not "implement measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers through the Tower Web site."

Key Lesson If a company makes a general promise to take reasonable steps to secure customer information, the FTC will expect that its data security measures will anticipate commonly known vulnerabilities. A company's failure to adopt such safeguards could attract FTC scrutiny, even if the company had not exposed payment card data or highly sensitive information.

1.1.6.3.2 Ensure that Security Controls are Sufficient to Abide by Promises about Security and Privacy

***In the Matter of Twitter, Inc.,* Docket No. 4316 (2011)** Social media company Twitter collects a great deal of nonpublic information about its users, including IP addresses, email addresses, and mobile phone numbers. The site also enables users to exchange nonpublic direct messages, and to make certain tweets nonpublic. In its privacy policy from 2007 to 2009, Twitter's privacy policy stated that it employs "administrative, physical, and electronic measures designed to protect your information from unauthorized access." The policy also stated that direct messages "are not public; only author and recipient can view direct messages" and that users can switch the status of their accounts to "protected" in order to "control who is able to follow them, and keep their updates away from the public eye." The FTC alleged that Twitter failed to enact controls that would enable them to live up to this promise. For instance, the FTC alleged that the company "granted almost all of its employees the ability to exercise administrative control of the Twitter system, including the ability to: reset a user's account password, view a user's nonpublic tweets and other nonpublic user information, and send tweets on behalf of a user. Such employees have accessed these administrative controls using administrative credentials, composed of a user name and administrative password." Moreover, the FTC

alleged that Twitter failed to require complex administrative passwords, prohibit employees from storing administrative passwords in their personal email folders, disable accounts after a certain number of unsuccessful attempts, and require password changes after a specified period of days. In 2009, hackers used unsecured administrative accounts to access users' nonpublic information, reset their passwords, and send public tweets from these accounts. For instance, one hacker accessed Barack Obama's Twitter account and offered his followers the chance to win $500 in gasoline if they completed a survey. The FTC alleged that Twitter "did not use reasonable and appropriate security measures to prevent unauthorized access to nonpublic user information."

Key Lesson A company must ensure that its administrative accounts have adequate controls to enable it to abide by all of the promises about data security that it makes in its privacy policy and other public statements. Employees should not have robust administrative accounts as default; instead, employees only should have the authorization that is necessary for them to perform their jobs.

***In the Matter of Upromise,* Docket No. C-4351 (2012)** Upromise is a membership-based service that teams with merchants and provides online deals to customers that sign up for its service. Among its services is the Upromise TurboSaver toolbar, which promotes Upromise merchant partners in customers' search results and personalizes offers to customers based on their web-browsing information. The tool collected web-browsing information, as well as the data that customers entered into web pages. The Upromise TurboSaver privacy policy stated that the toolbar would only "infrequently" collect personal information, that a Upromise filter "would remove any personally identifiable information" before the data is transmitted, and that Upromise would make "every commercially viable effort … to purge their databases of any personally identifiable information." The Upromise security statement separately promised that Upromise "automatically encrypts your sensitive information in transit from your computer to ours." The FTC alleges that Upromise never prevented the toolbar from collecting and transmitting personal information such as PIN numbers, credit card numbers, and expiration dates. For example, assume that a customer was entering bank account information on a bank website. Even if the bank's website employed the necessary SSL encryption technology, the Upromise toolbar allegedly would transmit that data via clear text, thus defeating any security protections that the bank's website had provided to this sensitive information. An external security researcher in 2010 announced that this information was collected by Upromise and conveyed via clear text. In its complaint against Upromise, the FTC alleged that the company "created unnecessary risks of unauthorized access to consumer information by the Targeting Tool transmitting sensitive information from secure web pages, such as financial account numbers and security codes, in clear readable text over the

Internet," and that the company "failed to use readily available, low-cost measures to assess and address the risk that the targeting tool would collect such sensitive consumer information it was not authorized to collect."

Key Lesson If a company promises to protect and encrypt information, the FTC will hold it accountable if it fails to do so. Moreover, the Upromise case is one of many in recent years in which the FTC has brought a complaint after an independent security researcher has discovered and announced a company's security vulnerability. A number of such researchers have obtained large followings on the Internet, and their findings can prompt immediate and severe regulatory action.

1.1.6.3.3 Omissions about Key Security Flaws also can be Misleading

***In the Matter of Oracle Corporation,* Docket No. C-4571 (2016)** Oracle makes Java, the software that enables consumers to use a variety of online programs. Java has long been known for being the target of hackers, and Oracle routinely releases updates to patch vulnerabilities. Oracle typically delivered these updates to consumers via a pop-up prompt, and when the consumer installed the update, Oracle informed the consumer that "Java provides safe and secure access to the world of amazing Java content," and informed the customer that the computer would have the latest "security improvements." Unfortunately, even if the consumer installed the update, the older, vulnerable Java version remained on the consumer's computer. The FTC brought a complaint against Oracle, alleging that it should have informed customers that updating Java still left their computers vulnerable unless they removed the older Java versions. In the complaint, the FTC alleged that by "failing to inform consumers that the Java SE update process did not remove all prior iterations of the software, Oracle left some consumers vulnerable to a serious, well-known, and reasonably foreseeable security risk that attackers would target these computers through exploit kits, resulting in the theft of personal information[.]"

Key Lesson If a company is aware of a major security vulnerability that could expose consumer information, it should disclose that vulnerability – and ways to fix it.

1.1.6.3.4 Companies Must Abide by Promises for Security-Related Consent Choices

***In the Matter of HTC America, Inc.,* Docket No. C-4406 (2013)** HTC manufactures Windows- and Android-based smartphones. The FTC's complaint against HTC focused primarily on HTC's Android-based phones. Android, which is Google's operating system, has a "permission-based security model" that requires a customer to explicitly provide a third-party application with permission before that application can access that customer's sensitive information (e.g., geolocation information or payment card data). HTC's user manual for its Android devices stated that apps "may require access to your personal

information (such as your location, contact data, and more) or access to certain functions or settings of your device" and that during installation, a screen "notifies you whether the app will require access to your personal information or access to certain functions or settings of your device. If you agree to the conditions, tap OK to begin downloading and installing your app." As the FTC concluded, this statement led consumers to believe that "through the Android permission-based security model, a user of an HTC Android-based mobile device would be notified when a third-party application required access to the user's personal information or to certain functions or settings of the user's device before the user completes installation of the third-party application." However, the FTC alleges that HTC devices contained numerous security vulnerabilities that prevented such notice and consent. For instance, HTC had circumvented the Android permission model through a number of "permission re-delegation" vulnerabilities, which occurs when one app that has permission to access sensitive information transfers that permission to another app, even if the consumer has not provided consent for that second app to obtain the information. Separately, the FTC alleged that HTC allowed customers to install apps that were not downloaded through the Android app store, creating another avenue for third-party apps to circumvent the notice-and-consent process that Android requires. Those shortcomings, along with other vulnerabilities in HTC devices, meant that "third-party applications could access a variety of sensitive information and sensitive device functionality on HTC Android-based mobile devices without notifying or obtaining consent from the user before installation," the FTC alleged in its complaint against HTC.

Key Lesson As with the Fandango case, the FTC takes a very aggressive stance against companies that actively disable security settings that are provided as the default by app stores or operating systems. As online life increasingly moves from the traditional web to apps, the security policies of intermediaries such as app stores will play an increasingly important role in determining whether an app or device-maker's security practices are unfair under Section 5.

1.1.6.3.5 Companies that Promise Security Must Ensure Adequate Authentication Procedures

***In the Matter of Trendnet, Inc.,* Docket No. C-4426 (2014)** Trendnet manufactures and sells a number of connected devices, including SecurView IP-connected cameras, which enable users to install cameras in their homes (e.g., in a baby's room) and view the video live on the Internet. SecurView's website allows its users to choose whether to require a log-in or password to access the live video (because in some cases, users may want a live video to be publicly accessible). For those who did not want the video to be available to the public, Trendnet assured them that the system was secure. Indeed, SecurView's packaging contained a sticker with a padlock and the word "security." However, from April 2010 to February 2012, 20 models of Trendnet's camera allegedly did not require

log-in credentials, even if users had chosen to require them. In other words, any member of the public could access *any* of the camera feeds. Indeed, hackers posted links to live feeds of almost 700 Trendnet cameras, publicly displaying scenes such as babies asleep in cribs and children playing. The FTC took this breach particularly seriously, stating that it "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 families, including young children, will be observed and recorded by strangers over the Internet." The FTC asserted that 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."

Key Lesson The Trendnet case was a particularly newsworthy complaint due to the sensitive nature of the information that was disclosed. However, from a legal standpoint, perhaps the biggest lesson from the case is that if a company markets a product or service as "secure" (and, in fact, includes "secure" in the name of its product), then the FTC is far more likely to scrutinize its practices if later there is a security vulnerability.

1.1.6.3.6 Adhere to Promises about Encryption

***In the Matter of Credit Karma, Inc.,* Docket No. C-4480 (2014)** Credit Karma provides a mobile app that allows customers to view their credit reports and scores. The company's app privacy policy stated that it uses SSL "to establish a secure connection between your computer and our servers, creating a private session." Apple, which manufactures the iPhone and provides the iOS operating system, provides application programming interfaces that, by default, use encrypted SSL communications. Apple warns developers that disabling this default setting "eliminates any benefit you might otherwise have gotten from using a secure connection. The resulting connection is no safer than sending the request via unencrypted HTTP because it provides no protection from spoofing by a fake server." Credit Karma allegedly overrode those default settings and therefore did not use SSL communications. Accordingly, the FTC alleged, "attackers could, in connection with attacks that redirect and intercept network traffic, decrypt, monitor, or alter any of the information transmitted from or to the application, including Social Security numbers, dates of birth, 'out of wallet' information, and credit report information." Moreover, the FTC alleged that hackers could "intercept a consumer's authentication credentials, allowing an attacker to log into the consumer's Credit Karma web account to access the consumer's credit score and a more complete version of the credit report." The FTC asserted that misuse of this information "can lead to identity theft, including existing and new account fraud, the compromise of personal information maintained on other online services, and related consumer harms."

Key Lesson As with the Fandango and HTC cases, here the FTC had little tolerance for a company that circumvented a mobile operating system's default security settings. Such settings are quickly becoming the de facto standard of care for mobile app security.

1.2 State Data Breach Notification Laws

At the state level, perhaps the most pervasive cybersecurity-related laws are data breach notification laws. Forty-seven states and the District of Columbia have enacted such laws, which require companies and government agencies to notify consumers, regulators, and credit bureaus about data breaches under specified circumstances.

Companies must be aware of every breach notification law, even if it does not have any employees or property in that state. Each breach notification law applies to the unauthorized disclosure of that state's residents. For example, if a California company discloses the personal information of New York residents, the New York law will determine whether and how the company is required to notify consumers, regulators, and credit bureaus. As a practical matter, because companies often process data about customers and other individuals who are located across the United States, they are subject to all 48 breach notification laws in the United States.

Determining whether a company's breach notice obligations are triggered can be quite time-consuming because this determination requires a careful review of the facts of the data breach. Although many of the state laws have similar provisions – indeed, some contain identical phrases and requirements – there are important differences. Because of these deviations among breach notification laws, quite often, a company is required to report a data breach under the laws of some states but not under the laws of others.

If companies do not properly issue data breach notifications, they face significant fines and private litigation in many states. Yet, they must fulfill these legal obligations during a chaotic period after a data breach, when they often have incomplete information about the incident. Companies must balance their legal duties to disclose with the equally compelling need to ensure that their disclosures are accurate. If a company incorrectly describes a data breach, it could face an action from a state regulator or the FTC under Section 5, discussed in Section 1.1.1 of this chapter. Moreover, a company's initial breach disclosures could have a significant impact on the company's brand and public relations.

This Section provides an overview of the key elements of breach notification laws. The first subsection examines the circumstances under which state laws require companies to issue data breach notifications to customers. The second

subsection outlines the required contents of the customer notifications. The third subsection examines companies' obligations to notify state regulators and credit bureaus. The fourth subsection examines the penalties and litigation that companies can face if they do not comply with the statutes.

This section discusses the most common rules under the state data breach notification statutes, and also notes many of the state laws that differ from these default rules. However, many of these state laws are unique and contain particular requirements that vary considerably, so companies should always consult the current version of the states' data breach notification law to understand the precise requirements in each state. For ease of reference, a summary of all 48 U.S. data breach notification laws, current as of 2016, is published in Appendix B.

Keep in mind that certain industries that process highly sensitive data – including healthcare companies and financial institutions – *also* face breach notification requirements under federal law, discussed in Chapter 3.

1.2.1 When Consumer Notifications are Required

After many data breaches, the state breach notification laws do not require companies to notify customers, regulators, or credit bureaus. In many cases, the information that was compromised is not covered by the state laws, and therefore notification is required. Moreover, every state except Tennessee does not require notification if the breached personal information was encrypted and the encryption key was not disclosed. There also are a number of exceptions that allow companies to avoid breach notifications even if unencrypted personal information was accessed without authorization, including provisions in most laws that allow companies to withhold notifications if they determine that the disclosure will not create a reasonable likelihood of harm to the customers.

Even if companies are not required to notify a state's residents of a data breach, many do so anyway. Many companies view breach notifications as a matter of good business and transparency. Moreover, if a company is required to notify residents in even one state, news of the breach may be quickly reported in the media. That would leave customers in other states wondering whether their information also was compromised, and questioning why the company did not notify them.

1.2.1.1 Definition of Personal Information

State data breach laws only apply to unauthorized acquisition of *personal information*, a term that is defined in each statute. If a data breach only exposes data that does not fall under the statute's definition of "personal information," then a company is not required to notify customers. In many cases, data that is not classified as "personal information" still may be quite

sensitive and valuable to identity thieves or other criminals, but the notification rule does not apply.

In nearly every state with a data breach law, the definition of personal information includes, at minimum, an individual's first name or initial and last name, in combination with at least *one* of the following categories of information: (1) Social Security number; (2) driver's license or state identification number; or (3) account number, credit card number, or debit card number, along with any required password or access code.

In addition to those three elements, a number of other states include elements that, combined with an individual's name, trigger a data breach requirement (specific definitions for each state, as of mid-2016, are summarized in Appendix B):

Medical information: Arkansas, California, Florida, Missouri, North Dakota, Oregon, Texas
Health insurance information: California, Florida, North Dakota, Oregon
Online account information (including username and unencrypted password): California, Florida
Biometric data (e.g., fingerprints): Iowa, Nebraska, North Carolina, Oregon, Wisconsin
Taxpayer identification number: Maryland, North Carolina
Tribal identification number: Montana, Wyoming
Any federal or state identification number: Wyoming
Date of birth: North Dakota
Mother's maiden name: North Dakota
Employment identification number: North Dakota
Passport number: North Carolina, Oregon
Digital signature: North Carolina, North Dakota

A handful of states also require notification of the unauthorized access to information even if the individual's names are not disclosed. California and Florida require notification for the disclosure of a user name or email address, in combination with a password or security question and answer that would allow access to an online account. Maine and Oregon require notification of the breach of certain categories of information, without the individual's name, if the information could be used for identity theft. Texas requires notification for the disclosure of any information related to an individual's healthcare, even if it is not disclosed with the individual's name.

Many breach notification laws explicitly state that they do not cover information that is lawfully made public by the government or media.

1.2.1.2 Encrypted Data

All state data breach notification laws, except Tennessee's, do not require notification of the breach of personal information that is encrypted. Most of these

laws do not provide technical specifics for encryption; however, Massachusetts requires encryption with at least a 128-bit processed. Additionally, many of the state encryption exceptions only apply if the encryption key was not accessed. In 2015, Tennessee amended its breach notification law and became the first and only state to require notification even if the personal information was encrypted. This change had a significant impact nationwide and caught many data security professionals by surprise. Until this change, companies that properly encrypted their data could avoid any notification obligation; now, encryption does not fully absolve companies of this obligation. However, Tennessee still has an exception to the notice requirement if the company determines that the breach did not create a risk of harm – discussed below. Companies would have a very strong argument that if all of the personal data was encrypted, a breach would not pose a risk of harm.

1.2.1.3 Risk of Harm

In thirty-eight of the states with breach notification laws, companies can avoid notification obligations if, after investigating the breach, they determine that the incident did not create a risk of harm for individuals whose personal information was exposed. The exact wording of this exception varies by state. For example, in Michigan, companies are not required to notify individuals if they determine that "the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft" with respect to Michigan residents. Oregon's exception is a bit narrower, applying if the company "reasonably determines that the consumers whose personal information was subject to the breach of security are unlikely to suffer harm." New York's exception only applies if the company determines that the breach did not compromise the security, confidentiality, or integrity of the personal information. Florida's risk-of-harm exception only applies if the company provides to the Florida Department of Legal Affairs its written determination that the disclosure will not result in harm, and retains that determination for five years.

Ten of the data breach notification statutes do not have risk-of-harm provisions, and therefore require notification regardless of whether the company concludes that the breach is likely to lead to harm to individuals. These "strict liability" jurisdictions are California, the District of Columbia, Georgia, Illinois, Massachusetts, Maine, Minnesota, Nevada, North Dakota, and Texas.

1.2.1.4 Safe Harbors and Exceptions to Notice Requirement

Most states have some additional, narrow exceptions to the breach notification rules. Commonly, if a company follows the breach notification procedures of its own information security policy, then it does not have to notify consumers pursuant to the specific requirements of the state law, as long as the timing of

its notice is consistent with the state law. Additionally, many states allow regulated financial institutions and healthcare providers to notify consumers under applicable federal laws and regulations, rather than following the state breach notice provisions.

1.2.2 Notice to Individuals

The U.S. breach notification process is not one-size-fits-all. State laws differ as to the timing of the notices, the form in which they can be delivered, and the content of the notices. Failure to comply with these technical requirements can lead to liability, so companies are wise to double-check the current version of each state's breach notification law to ensure that they are providing proper notice.

1.2.2.1 Timing of Notice

Most breach notification laws require companies to notify customers as expediently as possible and without unreasonable delay, although the exact wording of that requirement varies by state (and is summarized by state in Appendix B). Although these states do not require notification within a specified number of days after discovering the breach, state regulators likely will not tolerate an unjustified delay of more than a month or two.

Eight states require notice within a specified period after discovery of the breach. The shortest time frame is in Florida, which requires individual notice within 30 days of discovery of a breach. Ohio, Rhode Island, Tennessee, Washington state, Wisconsin, and Vermont require notice within 45 days, and Connecticut requires notice within 90 days of discovery of a breach.

All breach notification laws allow companies to delay notification if the delay would harm an ongoing law enforcement investigation. Many of the laws also allow companies to delay notice to determine the scope of the breach, identify affected individuals, and restore the confidentiality, integrity, and availability of the company's computer systems and data.

1.2.2.2 Form of Notice

Companies also must ensure that they deliver the notice in a medium that is approved by each statute. The breach notification laws all allow written notice, mailed to the last known address on record for the individual. The laws also typically allow electronic notice delivered via email to the last known email address that the company has on record. Some states only allow electronic notice if email was the primary method of communication between the company and customer. The states also generally only allow electronic communication if the company obtained valid consent to delivery electronic notices pursuant to the federal E-SIGN Act. About half of the statutes also allow

companies to deliver the notices via telephone, and a handful also allow notice to be delivered via fax machine.

Additionally, state breach notification laws allow companies to provide "substitute" notice if the company does not have sufficient contact information to deliver the other forms of notice, if the total cost of notification would exceed an amount specified in the statute, or if the company would be required to notify more than a certain number of people specified in the statute. Substitute notice generally consists of three elements: (1) email notice to any individuals for whom the business has an email address on file; (2) if the company has a website, conspicuous notice of the breach on the site; and (3) notice to major statewide media.

1.2.2.3 Content of Notice

Most state breach notification laws do not require a breach notice to contain specific information. A minority of states, however, require notices to individuals to contain certain statements or data. These requirements are listed in detail, by jurisdiction, in Appendix B. Among the most common requirements are:

- contact information for the company;
- a general description of the breach;
- the categories of personal information compromised in the breach;
- the date(s) of the breach;
- contact information for major credit bureaus, the state attorney general, and the Federal Trade Commission;
- advice to remain vigilant about identity theft by reviewing financial account records and credit reports; and
- information about identity theft protection services (California and Connecticut require companies to provide the services for 12 months).

Some states prohibit individual notices from containing certain types of information. For instance, Illinois prohibits companies from notifying individuals of the number of Illinois residents whose data was compromised. Massachusetts also prohibits companies from stating the number of state residents affected, and it also bars companies from describing the nature of the breach.

1.2.3 Notice to Regulators and Consumer Reporting Agencies

If a company notifies individuals about a data breach, it also may be required to notify state regulators or the three major credit bureaus.

Eighteen states (listed in Appendix B) require companies to notify state officials – typically the Attorney General – if individuals were notified. In six of those states, regulator notification is required only if the number of individuals

notified exceeds a specified threshold (typically 500 or 1000 state residents). About half of these states require the regulator notice to contain specific content, such as a general description of the breach, the number of the state residents affected, and the steps that the company has taken to remediate harm. Some statutes require companies to provide regulators with samples of the notices that were sent to individuals. Some states, including California, New York, and North Carolina, provide companies with a form to complete.

Most – but not all – states also require notification of the major credit bureaus (Experian, EquiFax, and TransUnion). Typically, credit bureau notification is only required if more than 1000 residents of the states have been notified, though some have higher thresholds. The breach notice laws often require companies to inform the credit bureaus of the date that the notices were sent to individuals.

1.2.4 Penalties for Violating State Breach Notification Laws

Typically, state attorneys general may bring enforcement actions against companies that fail to comply with their states' data breach notification laws. Although the remedies vary by state, the officials typically can seek injunctions ordering disclosure of the breach and civil fines. In fourteen states[48] and the District of Columbia, individuals can bring private lawsuits seeking damages, often under state consumer protection statutes.

1.3 State Data Security Laws

Twelve states have enacted statutes that impose data security requirements on companies that own or process personal information from the states' residents. As with the data breach notification laws, the location of a company's headquarters is irrelevant to determining whether these laws apply to the company. Instead, a state's data security law will apply if a company owns or processes personal information of even one resident of that state. Because most mid-sized and large companies process the personal information of residents of all fifty states, companies must pay attention to the requirements of all state data security laws.

Of the twelve data security laws, eight are relatively flexible, requiring companies to implement reasonable security procedures, but not specifying precisely

48 The jurisdictions that allow private parties to sue for violations of data breach notification statutes are Alaska, California, Hawaii, Louisiana, Maryland, Massachusetts, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Virginia, Washington state, and the District of Columbia.

what constitutes "reasonable." Those states are Arkansas,[49] California,[50] Connecticut,[51] Florida,[52] Indiana,[53] Maryland,[54] Texas,[55] and Utah.[56]

A note about statutes, laws, regulations, and government guidelines described throughout this book: when possible, we use the language directly from the original text. However, for brevity and clarity, some of these descriptions are shortened or modestly edited. Moreover, Congress and state legislatures occasionally amend data security requirements. Accordingly, before citing any of these laws in an official document, consult the primary source, which is accessible via the citation in the footnotes.

1.3.1 Oregon

Oregon's data security law, which was significantly revised in 2015, also requires companies that own or possess Oregon consumers' personal

---

49 Ark. Code. 4-110-104(b) ("A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall 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.").

50 Cal. Civ. Code 1798.81.5 ("A business that owns, licenses, or maintains personal information about a California resident shall 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.").

51 Conn. Pub. Acts No. 08-167(a) ("Any person in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal.").

52 Fla. Stat. 501.171(2) ("Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.").

53 Ind. Code 24-4.9-3-3.5 ("A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.").

54 Md. Code Com. Law 14-3503(a) ("To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.").

55 Tex. Bus. & Com. Code 48.102(a) ("A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.").

56 Utah Code 13-44-201(a) ("Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to … prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business[.]").

information to develop and implement reasonable safeguards.[57] However, the Oregon law provides more detail about how companies can satisfy the requirement.

Under the Oregon law, the company could satisfy the "reasonableness" requirement by developing an information security plan that contains the following safeguards:

- Administrative safeguards, such as:
  - designating a coordinator for the security program;
  - identifying "reasonably foreseeable" internal and external risks;
  - assessing if existing safeguards control those risks;
  - training and managing employees in security;
  - selecting service providers that can maintain safeguards, and requiring them, by contract, to maintain the safeguards; and
  - adjusting the security program when necessary.
- Technical safeguards, such as:
  - assessing risks in network and software design;
  - assessing risks in information processing, transmission, and storage;
  - detecting, preventing, and responding to attacks or system failures; and
  - testing and monitoring regularly the effectiveness of information security safeguards.
- Physical safeguards, such as:
  - assessing risks of information storage and disposal;
  - detecting, preventing, and responding to intrusions;
  - protecting against unauthorized access during or after collecting, transporting, destroying, or disposing of the personal information; and
  - disposing of personal information after it is no longer needed for business or legal purposes by adequately destroying it so it cannot be read or reconstructed.[58]

Alternatively, companies could satisfy the Oregon law by complying with the Gramm-Leach-Bliley Act (if the company is a financial institution),[59] the Health Insurance Portability and Accountability Act (if the company is subject to HIPAA),[60] or a state or federal law that provides greater protection to personal information than the procedures.[61]

---

57 O.R.S. 646A.622(1) ("A person that owns, maintains or otherwise possesses data that includes a consumer's personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the information.").

58 O.R.S. 646A.622(2)(d).

59 O.R.S. 646A.622(2)(b).

60 O.R.S. 646A.622(2)(c).

61 O.R.S. 646A.622(2)(a).

1.3.2 Rhode Island

Rhode Island's data security law, which, like Oregon's, was amended significantly in 2015, requires state agencies and firms to have "reasonable security procedures and practices."[62] The statute requires the program to be appropriate to:

- the size and scope of the organization;
- the nature of the information; and
- "the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information."[63]

Rhode Island prohibits organizations from retaining personal information for a period longer than is reasonably required to provide requested services, to meet the purpose for which the personal information was collected, or in accordance with a written retention policy or as required by law.

Organizations that disclose Rhode Island residents' personal information to third parties (e.g., service providers) must require those third parties, by contract, to implement and maintain reasonable security procedures and practices.

1.3.3 Nevada

Nevada requires data collectors that maintain records containing Nevada residents' personal information to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."[64] Companies that disclose Nevada residents' personal information to service providers must contractually require those companies to adopt reasonable security measures.

Nevada's data security law is unique in that it requires companies to use encryption before either (1) electronically transferring Nevada residents' personal information or (2) moving any data storage device containing Nevada residents' personal information beyond the logical or physical controls of the data collector, its data storage contractor, or, if the data storage device is used by or is a component of a multifunctional device, a person who assumes the obligation of the data collector to protect personal information.[65] The encryption requirements do not apply to telecommunications providers acting solely in the role of conveying communications of other persons.[66]

---

62 R.I. Gen. Law 11-49.3-2(a).
63 *Id*.
64 N.R.S. 603A.210.
65 N.R.S. 603A.215.
66 N.R.S. 603A.215(4).

Nevada's statute does not provide specific technological requirements for encryption to satisfy this requirement. The statute states that the technology could be one that was adopted by a standards-setting body, such as the Federal Information Processing Standards issued by the National Institute of Standards and Technology.[67] The encryption also should use "[a]ppropriate management and safeguards of cryptographic keys to protect the integrity of the encryption" using guidelines that have been published by a standards-setting body, such as NIST.[68]

Nevada also requires data collectors that accept payment card information to comply with the Payment Card Industry Data Security Standard (PCI DSS), which is explained in Chapter 3 of this book. Although companies that accept payment card information typically must comply with PCI DSS due to contractual requirements with credit card companies, Nevada's law is unique in that it requires companies, by law, to comply.

1.3.4 Massachusetts

Massachusetts has enacted the most detailed and comprehensive general data security requirements in the United States. These requirements have quickly become de facto national standards for mid-sized and large businesses that have customers nationwide, as they most likely process some personal information of Massachusetts residents.

Massachusetts' data security law requires the state's Department of Consumer Affairs and Business Regulation to adopt data security regulations to safeguard Massachusetts residents' personal information. The statute requires the regulations to:

- "insure the security and confidentiality of customer information in a manner fully consistent with industry standards";
- "protect against anticipated threats or hazards to the security or integrity of such information"; and
- "protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.[69]"

The Massachusetts Department of Consumer Affairs issued comprehensive data security regulations[70] to comply with this mandate. The regulations, modestly edited below for clarity and brevity, require every company and person who owns or licenses personal information about a Massachusetts resident to develop a comprehensive written information security program

67 N.R.S. 603A.215(5)(b).
68 *Id.*
69 Mass. Gen. Law 93H § 2(a).
70 201 C.M.R. 17.00 et seq.

that contains administrative, technical, and physical safeguards that are appropriate to:

- the size, scope, and type of business of the company;
- the amount of resources available to the company;
- the amount of stored data; and
- the need for security and confidentiality of both consumer and employee information.[71]

The Massachusetts regulations are unique in their specificity of the *required* components of a written information security plan. The regulations require all information security plans to include the following:

- At least one employee who is designated to maintain the security program.
- Identification and assessment of reasonably foreseeable internal and external risks to security, confidentiality, and integrity of records that contain personal information.
- Evaluating and improving the effectiveness of the current safeguards for limiting the risks, including but not limited to
  - ongoing employee training,
  - employee compliance with information security policies and procedures, and
  - means for detecting and preventing security system failures.
- Developing records storage, access, and transportation security policies.
- Disciplinary measures for information security violations.
- Preventing terminated employees from accessing personal information.
- Overseeing service providers that have access to consumers' personal information by
  - taking "reasonable steps" to select and retain providers that can maintain adequate security measures, and
  - contractually requiring service providers to maintain appropriate security measures.
- Reasonably restricting physical access to personal information.
- Regular monitoring to ensure proper operation of information security program.
- Reviewing scope of security measures at least annually or whenever there is a material change in business practices.
- Documenting responsive actions after a breach.[72]

71 201 C.M.R. 17.03(1).
72 201 C.M.R. 17.03(2).

The Massachusetts regulations also require information security programs to contain the following technical security measures when feasible:

- Secure user authentication protocols, including
  - control of identifiers,
  - a "reasonably secure" method of assigning passwords and other access mechanisms,
  - control of storage of passwords,
  - restricting access to active user accounts, and
  - blocking access to log-ins after multiple unsuccessful log-in attempts.
- Secure access control measures that
  - restrict access to personal information to those who need the information to perform their jobs, and
  - assign unique identifications plus passwords that are not default credentials and are reasonably designed to maintain integrity of access controls.
- Encryption of all personal information that travels across public networks or is transmitted wirelessly or stored on laptops or portable devices.
- Reasonable monitoring for unauthorized use.
- Up-to-date firewall protection and operating system patches.
- Reasonably up-to-date malware protection and anti-virus software.
- Employee computer security training.[73]

The Massachusetts regulations are, by far, the most detailed general data security requirements in the United States. Despite the length of the regulations, they are not significantly more onerous than the general expectations that regulators long have had for companies that handle personal information. For instance, it is unlikely that the FTC would agree to allow a company to store personal information on unencrypted laptops, nor would the California Attorney General suggest that companies allow multiple employees to access personal information with a single log-in credential. The Massachusetts regulations merely spell out what is generally considered in the industry to constitute "reasonable" data security. Even if a company does not own or process personal information of Massachusetts residents, it would be well advised to use the Massachusetts regulations as guidelines for its own data security programs.

73 201 C.M.R. 17.04.

1.4 State Data Disposal Laws

Thirty-one states require companies to take reasonable steps to dispose of records that contain personal information.[74] Although the wordings of the laws vary by state, they generally require steps such as shredding or otherwise rendering the personal information unreadable or undecipherable, and preventing the information from being reconstituted. Nonetheless, most statutes do not provide much detail on the "reasonable measures" necessary to satisfy the requirements of data disposal laws.

Massachusetts provides some additional detail about the minimum standards for disposal of personal information. Paper records should be either "redacted, burned, pulverized or shredded" so that the personal information cannot be read or reconstituted, and nonpapermedia (e.g., electronic media) should be "destroyed or erased so that personal information cannot practicably be read or reconstructed."[75]

Hawaii's law provides some detail about the oversight of vendors that destroy information. It states that a business can satisfy this requirement by exercising "due diligence" over records destruction contractors. Due diligence consists of:

- reviewing an independent audit of the disposal business' operations and compliance with the state data disposal law;
- obtaining information about the disposal business from several references or other reliable sources and requiring the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review; or
- reviewing and evaluating the disposal business' information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the disposal business.[76]

---

74 Alaska Stat. 45.48.500 (Alaska); Ariz. Rev. Stat. § 44-7601 (Arizona); Ark. Code § 4-110-104 (Arkansas); Cal. Civ. Code 1798.81 (California); Colo. Rev. Stat. § 6-1-713 (Colorado); Conn. Gen. Stat. § 42-471 (Connecticut); Del. Code tit. 6 § 5002C (Delaware); Fla. Stat. § 501.171(8) (Florida); Ga. Code § 10-15-2 (Georgia); Haw. Rev. Stat 487R-2 (Hawaii); 815 ILCS 530/40 (Illinois); Ind. Code 24-4-14-8 (Indiana); Kan. Stat. § 50-7a03 (Kansas); Ky. Rev. Stat. § 365.725 (Kentucky); Mass. Gen. Laws Ch. 93I, § 2 (Massachusetts); Md. State. Gov. Code 10-1303 (Maryland); MCL § 445.72a (Michigan); Mont. Code § 30-14-1703 (Montana); Nev. Rev. Stat. § 603A.200 (Nevada); N.J. Stat. § 56:8-162 (New Jersey); N.Y. Gen. Bus. Law § 399-H (New York); N.C. Gen. Stat. § 75-64 (North Carolina); Ore. Rev. Stat. § 646A.622 (Oregon); R.I. Gen. Laws § 6-52-2 (Rhode Island); S.C. Code 30-2-190 (South Carolina); Tenn. Code § 39-14-150(g) (Tennessee); Tex. Bus. & Com. Code § 72.004 (Texas); Utah Code § 13-44-201(2) (Utah); 9 Vt. Stat. § 2445(b) (Vermont); Wash. Rev. Code § 19.215.020 (Washington state); Wisc. Stat. § 134.97 (Wisconsin).

75 Mass. Gen. Law Ch. 93I, § 2.

76 Haw. Rev. Stat. 487R-2.