The Law of Securing Consumer Data on Networked Computers

By Bret Cohen

The day before Thanksgiving 2013, Target was hacked. For the next 18 days, cybercriminals siphoned approximately 40 million credit and debit card numbers from point of sale systems as unaware holiday shoppers frequented the retailer's stores during its busiest time of the year.[1]

But the perpetrators may have laid the groundwork well before they started pilfering customer information from Target's systems. According to one report, two months earlier the thieves stole network credentials from one of Target's heating, air conditioning, and refrigeration vendors by infecting the vendor's computers through a virus-laden email.[2] With these credentials, they made their way into the company's payment system network a couple of weeks before the attack, where they planted and tested their malware.

Thickening the plot, Target may have been made aware of the attack as it was happening. Earlier in the year, the company purchased and installed sophisticated network security software that reportedly detected and alerted Target security specialists of the infiltration—twice—before the hackers began to transmit the stolen card data off of the company's network.[3] But Target did not act on those alerts, only putting an end to the leak after being notified by federal law enforcement officials.

Bret Cohen *practices in the Privacy and Information Management Group at Hogan Lovells in Washington, DC and blogs about data privacy and cybersecurity issues at* hldataprotection.com. *He can be reached at* bret.cohen@hoganlovells.com.

Target's story is hardly a unique one. As networked and cloud-based services have proliferated over the last decade, the increase in remote connectivity has led to a corresponding increase in hackers exploiting that connectivity for personal gain, and in organizations inadvertently exposing confidential information stored on their networks. In 2013 alone, Privacy Rights Clearinghouse, which compiles publicly reported breaches of sensitive personally identifiable information in the United States, collected information on 297 breaches that occurred due to hacking, malware, or an organization's unintended disclosure of data, including Target's.[4] Given the number of breaches that go unreported, the actual number certainly is much higher.

Despite the high number of breaches, the law has been slow to establish a duty of care for the security of consumer data stored on networked computers or other devices. A handful of lawsuits arising from such breaches have resulted in court opinions addressing the duty of care in specific contexts,[5] but the vast majority of breach suits have either been dismissed for lack of standing or failure to state a claim or, if surviving a motion to dismiss, are settled out of court.

To fill this void, a number of federal and state regulatory frameworks have developed in recent years to hold businesses responsible for protecting sensitive consumer data. Government regulators have used this authority to bring actions against businesses that suffer a breach of such consumer data which, in the eyes of the regulators, could have been prevented through the implementation of commercially reasonable data security measures.

THE FTC AS LEAD CONSUMER DATA SECURITY REGULATOR

The primary cop on the consumer data security beat has been the Federal Trade Commission (FTC). Since 2002, the FTC has brought and settled over 50 enforcement actions against businesses for allegedly maintaining insufficient data security practices, primarily under its authority to regulate "unfair or deceptive acts or practices in or affecting commerce" under Section 5 of the FTC Act.[6] Some states have contributed to the enforcement landscape as well under so-called Little FTC Acts, which grant them parallel and coextensive authority, as

well as a few state laws that provide more granular cybersecurity requirements.[7] But none has been as active, or has broken as much new ground, as the FTC. Therefore, this article focuses on the FTC's stated data security standards, as may be applied by the states as well.

The FTC typically proceeds under one of two theories. First, a business that fails to adopt industry-standard security measures to protect sensitive consumer information engages in "unfair" business practices. Second, a business that makes a promise that it will keep consumer data secure but then suffers a breach through inadequate safeguards commits a "deceptive" practice.

All of the FTC's Section 5 data security enforcements that have resolved to date have resulted in settlements, typically requiring companies to establish a comprehensive data security program and to conduct and file biennial, independent audits for 20 years.[8] Although these settlements are not accompanied by any financial penalty, any failure to comply with the settlement agreement over the next 20 years, including through another data breach due to a security lapse, can result in a penalty of $16,000 per record breached. A subsequent violation can be costly; in 2012, Google paid a $22.5 million penalty to settle its second Section 5 complaint in two years.[9]

Despite this robust enforcement environment, the FTC has not promulgated any regulations formally enumerating what data security practices it considers to be required by law. Instead, it issues complaints along with its settlements that indicate which of the settling organization's practices it considered inadequate. The FTC then encourages businesses to avoid these practices to reduce the risk of an investigation.[10]

Due to this uncertain and incremental enforcement approach, it is not always clear to businesses what security measures they need to implement to avoid violating the law.[11] This particularly is the case with respect to technical security measures used to secure remotely accessible networks and databases, where technology changes frequently and network compromises are common, if not expected, in some circumstances.

This article examines the FTC's complaints and informal guidance to clarify what network security measures the FTC believes are required legally by Section 5 of the FTC Act.[12]

WHAT TYPES OF CONSUMER DATA ARE COVERED?

The FTC does not treat all breaches equally. Consistent with the FTC's consumer protection mission, a key feature of the FTC's data security actions is that the breach leading to the investigation caused some sort of harm to consumers. In Section 5 unfairness cases, such harm also is an element of the offense, as a business practice can be considered "unfair" only if it "causes or is likely to cause substantial injury to consumers."[13] To date, nearly all of the FTC's Section 5 data breach actions have followed one of five different recurring fact patterns. Web site and network operators should therefore consider whether they adequately secure the categories of data reflected in these fact patterns.

By far, the most prevalent subject of FTC action in this space are breaches involving data that can be used by bad actors to commit fraud or identity theft.[14] Within this category, the FTC most frequently brings actions in the event of breaches of Social Security numbers or other government identifiers, payment card numbers, or financial account numbers, all of which can be used to withdraw money, spend money, or establish a financial account in a victim's name.

The second fact pattern involves the overcollection of consumer data without the knowledge of the consumer. While these FTC complaints also cite the exposure of certain data elements that can be used to commit identity theft, they focus on the comprehensiveness of the data collected. For example, in one action, the FTC scrutinized the information practices of a software application that, when installed, would:

> monitor nearly all of the Internet behavior that occurs on consumers' computers, including information exchanged between consumers and websites other than those owned, operated, or affiliated with respondent, information provided in secure sessions when interacting with third-party websites, shopping carts, and online accounts, and headers of web-based email; track certain non-Internet-related activities taking place on those computers; and transmit nearly all of the monitored information … to respondent's computer servers.[15]

Third, the FTC has brought actions when a hacker exploits a security vulnerability to gain access

to a consumer's online account and accesses sensitive information or makes changes to the account. For example, in a complaint against Twitter, the FTC criticized insufficient security measures that permitted intruders to "(1) gain unauthorized access to nonpublic tweets and nonpublic user information, and (2) reset any user's password and send unauthorized tweets from any user account."[16]

Fourth, the FTC has proceeded in a few cases against breaches of categories of information considered to be sensitive but not related to identity theft or any risk of financial harm, such as health-related information.[17] While there are not too many of these cases, the FTC in a number of published materials has mentioned other types of "sensitive" data categories in the same breath as fraud-facilitating and health information, including children's information and geolocation information.[18] It is not hard to imagine the FTC bringing a Section 5 claim focusing on breaches of these and other sensitive types of consumer data as well.

Finally, as a catchall, the FTC and state attorneys general have proceeded on the basis of a breach of certain consumer data when an organization has represented, explicitly or implicitly, that it will secure that data.[19]

Therefore, Web sites and companies that make available networked databases that collect, use, and store these sensitive types of consumer data, for example, online retailers who collect and process credit card payments, companies that collect Social Security numbers as part of a consumer identification process, and online services collecting health information, are at a greater risk for enforcement based on deficient cybersecurity measures.

THE LEGAL STANDARD

Typically, an investigation under Section 5 or a state Little FTC Act is precipitated by a report of a prominent security breach. Such reports have increased in frequency over the last decade as almost all states have enacted laws requiring organizations to report when they experience breaches of certain sensitive consumer information.[20] During the investigation, the FTC or state attorney general will examine the cause of the breach, often evaluating the company's entire cybersecurity program to determine if it was sufficient to protect the consumer data at issue. If, in the regulator's estimation, the company's security measures taken together were not "reasonable and appropriate," the regulator typically considers the lack of such measures, as a whole, to be a violation of the applicable consumer protection law.[21]

This test is extremely broad and gives regulators great latitude to adapt the standard to meet their determination of reasonableness based on any given set of facts.[22] Although the FTC has not put forward any formal guidance as to what security practices it considers to be reasonable, at the core of the "reasonableness" inquiry is a set of baseline standards that are derived from industry-standard cybersecurity practices.[23] Some of these standards are factored into the practices that the FTC considers "unreasonable" in its complaints. The FTC has also published an informal brochure, *Protecting Personal Information: A Guide for Business*, which sets forth at a high level some of the FTC's cybersecurity expectations.[24]

This section identifies the cybersecurity practices in complaints filed by the FTC and incorporated into its informal guidance that apply to consumer data stored on Internet-connected or other networked computers. These practices, which form the *de facto* legal standard followed by the FTC and many state regulators, can be grouped into four general categories: (1) testing and monitoring for reasonably foreseeable vulnerabilities and threats, (2) network architecture, (3) encryption, and (4) access control and authentication. Any company that relies on networked access to resources and consumer data, which includes cloud service providers, businesses that allow remote access to company databases and documents by employees or contractors, and just about any company with a Web site, should consider incorporating these practices into its security program to mitigate the risk of a regulatory action accusing it of failing to appropriately safeguard networked consumer data.

TESTING AND MONITORING FOR REASONABLY FORESEEABLE VULNERABILITIES AND THREATS

The FTC understands that networks and systems have vulnerabilities, and does not prosecute the existence of every vulnerability that might lead to a breach of consumer data. What it does not condone,

however, is when an organization fails to take steps to identify and remediate reasonably foreseeable risks, and then suffers a breach due to an exploitation of those unaddressed risks.

From the FTC's perspective, businesses that handle sensitive consumer data have an obligation to expend resources to detect risks that can be uncovered with "reasonable" effort and cost. It is less clear what levels are "reasonable"; in its business guide, the FTC notes that "[d]epending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit."[25]

In the context of the FTC's consent orders involving consumer data stored on networked computers, this general standard of care has been applied in four main forms.

The first is a requirement to test code and software for security vulnerabilities.[26] If the FTC thinks that a flaw could have been caught if there had been regular and diligent code testing and review, it will not give the developer the benefit of the doubt. While it is unclear what comprises the universe of "reasonably foreseeable risks" the FTC expects that code testing and review will catch, one category is for certain: the FTC expects businesses to test for well-known vulnerabilities and attacks. In the Web development context, two attacks that seem to particularly catch the FTC's attention are SQL injection and cross-site scripting attacks. In such attacks, a hacker tricks a Web site into executing administrative commands where the Web site was expecting other input, with the goal of retrieving sensitive data not intended to be disclosed by the Web site.[27] In addition, the FTC's business guide notes that Web developers should pay attention to the top Web development risks identified by the Open Web Application Security Project and SANS Institute, which also could be incorporated into the legal standard in the future.[28]

The second requirement is to implement an antimalware solution on the network and on endpoints with access to sensitive consumer data, and to regularly update it with vendor patches.[29] Despite the recent (and surprising) quote from leading antimalware provider Symantec that such software "is dead" because it catches less than half of modern cyberattacks,[30] the fact is that antimalware solutions are useful precisely because they catch those sorts of common attacks. Due to the ubiquity of antimalware packages, as well as their relative affordability, the FTC regards it as a necessary, if insufficient on its own, component of an effective data security program.

Third, in 2010, the FTC for the first time admonished a company for "fail[ing] to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization."[31] The complaint's inclusion of this requirement raised a number of eyebrows. While a system that monitors and blocks certain information from leaving networks (also known as a data loss prevention solution) is viewed as a valuable tool to help detect the exfiltration of sensitive data, it is not a solution categorically required by any industry standard. Data loss prevention solutions also can be very expensive to implement in practice. That said, the FTC in its business guide suggested that companies "[m]onitor outgoing traffic for signs of a data breach," watching "for unexpectedly large amounts of data being transmitted from your system to an unknown user" and, if detected, "investigat[ing] to make sure the transmission is authorized."[32] In 2012, the FTC entered into a consent order against a company that made sensitive consumer data available over a peer-to-peer network downloaded by an employee, arguing that the company's failure to "inspect[] outgoing transmissions to the internet to identify unauthorized disclosures of personal information" constituted an unreasonable security practice.[33] Therefore, companies who hold very sensitive consumer data on their networks—the breach in this case involved credit card numbers—should strongly consider the implementation of a data loss prevention solution.

Finally, the FTC has indicated that companies should maintain and regularly monitor network activity logs for indications of a breach.[34] Failing to do so is not likely to be the driving force of a regulatory enforcement action; it is more likely to be added to a complaint when there is a breach based on another deficient security practice that might have been detected sooner with regular log review. That said, to the extent that maintaining and monitoring logs can help determine the cause of a suspected breach, doing so can help a company (1) convince a regulator that a suspected breach was innocuous and (2) avoid

having to comply with state breach notification laws if the logs support the theory that the data was not exfiltrated, misused, or otherwise accessed without authorization.

NETWORK ARCHITECTURE

The previous section described data security processes that regulators expect businesses to use to detect security threats and vulnerabilities. This section describes some of the architectural features that companies are expected to build into their networks to reduce the likelihood of a breach, whether to protect against external threats or internal vulnerabilities.

The architectural feature most prominent in FTC complaints is the requirement to maintain and monitor effective network perimeter controls, such as firewalls, to block malicious content from entering the network.[35] The FTC's business guide dedicates an entire section to its expectations with respect to firewalls. Specifically, the FTC advises that companies should (1) use firewalls to protect networks from attacks while connected to the Internet or other public networks, (2) "[d]etermine whether" to install a "border" firewall (also known as a DMZ) to further insulate the main company networks where connected to the Internet, and (3) consider using internal firewalls where some machines on the network store more sensitive information than others.[36] Regardless of the strategy, at minimum industry-standard firewalls should protect servers containing sensitive consumer data from public networks.

Relatedly, the FTC has brought enforcement actions where fraud-facilitating consumer data, such as payment card data, resided on computers that were not segregated from other company systems that served nonsensitive functions or that permitted broader access rights.[37] Employing network or server partitions to insulate sensitive data from nonsensitive data—and to reduce the number of individuals who are able to access the sensitive partition, while enabling more robust authentication—creates another safeguard against a breach if a hacker is able to compromise the nonsensitive server but not the sensitive server.

The FTC has made clear that a business is responsible not only for securing its own network, but also for limiting the opportunities for insecure computers or other devices to connect to and access the network, and for technologically and contractually preventing third parties from accessing the network without meeting minimum security requirements.[38] For example, the FTC alleged in a recent complaint that a company did not maintain lawful security practices because it: (1) failed to ensure that third parties implemented adequate information security policies and procedures prior to connecting to the company's network; (2) permitted servers to connect to its network even though they used outdated operating systems that could not receive security updates or patches to address known security vulnerabilities; and (3) failed to adequately restrict third-party vendors' access to its networks and applications, such as by restricting connections to specified IP addresses or granting temporary, limited access.[39] To mitigate these risks, the business guide recommends that companies conduct an inventory of all connections to the computers and networks where they store sensitive consumer data, closing off connections where not needed (*e.g.*, by disabling or closing Internet-connected ports on a computer when an Internet connection is not necessary to perform its function).

ENCRYPTION

The FTC has addressed data encryption in two different contexts: (1) when sensitive consumer data is in transit, and (2) when it is at rest.

When sensitive consumer data is in transit over public networks (such as the Internet) or wireless networks, the FTC is unequivocal: it must be encrypted.[40] Doing so prevents others who may be monitoring the network from accessing and misusing the data. In its guidance and cases, the FTC describes several scenarios in which sensitive consumer data should be encrypted, including when transmitting data via an insecure file transfer protocol, via email, or through remote access to a network.[41] Functionally, this requires Web sites that collect sensitive consumer data over the Internet, such as e-commerce sites that accept credit card payments, to provide an encrypted connection such as through use of the Transport Layer Security or Secure Sockets Layer protocols. Web sites or other online services that claim they use

a secure connection, but which fail to properly implement it, risk FTC action.[42]

In contrast to the requirement to encrypt sensitive consumer data in transit, the FTC business guide recommends that businesses merely "consider" encrypting such information when stored on the network.[43] That said, the FTC has often cited a lack of encryption of data at rest as an unreasonable security practice when there has been another security failure that allowed the initial unauthorized access to the network.[44] So if there is unauthorized access to a database containing sensitive consumer data, a company can mitigate the risk of regulatory action (or a breach notification requirement) by having encrypted the database.

ACCESS CONTROL AND AUTHENTICATION

Not all data breaches are caused by a hacker infiltrating the system through the circumvention of a technical or code-based barrier. In some cases, sensitive consumer data is inadvertently made available through an Internet-facing or other public-facing network connection. In others, a hacker is given the keys to the kingdom in the form of crackable or easily accessible access credentials. The FTC treats both of these scenarios as "unreasonable," and therefore unlawful.

In the first scenario, a server storing sensitive data can be accessed without requiring the end user to enter access credentials. These authentication gaps can occur in a number of ways. For example, the FTC takes the position that a company violates Section 5 when it does not establish controls preventing its employees from downloading peer-to-peer file-sharing software that makes company files containing sensitive consumer data accessible to other members of the file-sharing network.[45]

The FTC also has proceeded against Internet-facing services that have failed to close backdoors that allowed Web users to access sensitive consumer data without being properly authenticated. In one case, a user exploited a "predictable resource location" flaw by typing a precise URL into the browser that gave the user access to an entire database containing customer information without being prompted for access credentials.[46] In another case, an e-commerce Web site's omission of an authentication code for its "order status" interface allowed any visitor to the site who entered a valid order number to exploit a "broken account and session management" vulnerability to view personal information relating to other consumers of the site.[47]

With respect to the second scenario, the FTC has brought actions against companies who experience breaches in part due to poor user credentialing procedures or substandard password requirements that allow hackers to guess valid credentials and gain access to user accounts. In its complaints and business guide, the FTC has given plenty of details about what credentialing and password shortcomings it considers to be part of a failure to provide "reasonable and appropriate" security,[48] including:

- not resetting default user IDs and passwords that are enabled on computer systems;
- not requiring customers or employees to use unique User IDs or "complex passwords" that "are difficult for hackers to guess," for example:
  - — by allowing remote access to a system developed by "Micros Systems, Inc.," using "micros" as both the user ID and the password;
  - — by not insisting that users choose passwords with a mix of letters, numbers, and characters;
- not prohibiting users from selecting the same word, including common dictionary words, as both password and user ID, or a close variant of the user ID as the password;
- not prohibiting the use of the same password across applications and programs;
- not requiring periodic changes of user credentials, "such as every 90 days," for customers and employees with access to sensitive personal information;
- not suspending user credentials after "a certain number of" or "a reasonable number of" unsuccessful login attempts;
- not using password-activated screen savers to lock employee computers after a period of inactivity;
- not locking out users who do not enter the correct password within a designated number of login attempts;
- permitting the sharing of user credentials among a customer's multiple users;
- allowing users to create new credentials without confirming that the new credentials were

created by customers rather than by identity thieves;
- not using two-factor authentication (*i.e.*, authentication using something tangible in addition to a password, such as a token, a key, or biometrics); and
- with respect to administrative credentials:
  - — not prohibiting the use of common dictionary words as administrative passwords;
  - — not requiring that administrative passwords be "unique," that is, different from any other password that the administrator uses to access third-party programs, Web sites, and networks;
  - — not prohibiting the storage of administrative passwords in plain text in email accounts;
  - — not providing an administrative login Web page that is made known only to authorized persons and is separate from the login Web page provided to other users; and
  - — not imposing other reasonable restrictions on administrative access, such as by restricting access to specified IP addresses.

Despite its length, this list of password "don'ts" is not too onerous to implement, with the possible exception of two-factor authentication, which can require the distribution of tokens and nontrivial reengineering of systems. That "requirement" was only mentioned in one complaint as an item on a longer list,[49] so the FTC may not even require it in all circumstances.

CONCLUSION

The vague-but-evolving cybersecurity standards set forth by the FTC in its complaints and business guide have been effective in influencing companies to invest in security programs designed to protect sensitive consumer data.[50] Under the prevailing legal framework, a business can be held responsible for a breach of sensitive consumer data if the breach resulted from a failure to implement "reasonable and appropriate" best-practice security measures to protect that data. But to avail itself of a defense that its security measures are reasonable and appropriate, a company needs to be able to demonstrate that its practices hold up to the prevailing industry standard. To do that requires the development and implementation of a compliance plan before any breach takes place.

Although the FTC's legal test for data security continues to develop, businesses and organizations handling sensitive consumer data on Internet-connected or other networked computers can take a number of steps to proactively avoid the threat of a regulatory action and to preserve the argument that they acted reasonably. The first step is complying with the security controls already identified by the FTC, many of which are described in this article, particularly in the areas of: (1) testing and monitoring for reasonably foreseeable vulnerabilities and threats, (2) network architecture, (3) encryption, and (4) access control and authentication. But in addition to those specific security controls, a company also can take the following steps to mitigate the risk of a regulatory data security action, a breach notification requirement, or a lawsuit:

1. **Take an inventory of sensitive consumer data, and connections to the servers containing that data.** The first step to avoiding a breach of regulated consumer data is to know what information the organization collects and maintains, where that information is stored, and how that information can be accessed. In many organizations, sensitive information may be scattered throughout systems and databases. Consider minimizing local copies of sensitive data, centralizing storage, minimizing access points, and encrypting sensitive data at rest.
2. **Minimize sensitive consumer data that is collected and stored.** Regulators usually step in only when a breach results in harm to consumers, and to date they only have viewed harm as arising from limited types of sensitive consumer data. So to the extent that a company does not need to collect or retain these types of consumer data on which regulators focus, limiting the collection and timely disposing of such data can mitigate the risk to the company. Given the risks involved, many companies outsource their processing of sensitive categories of consumer information over the Internet, such as by using third-party vendors to collect and process online credit card payments.
3. **Adopt a comprehensive data security program.** Corporate data security issues are not limited to

personally identifiable information, but also to proprietary and trade secret information as well. As a matter of good corporate hygiene, then, businesses may wish to establish and implement a comprehensive data security program that is reasonably designed to protect the security of all of the company's confidential information. A significant factor in convincing a regulator to decline to bring charges based on a breach is the level to which the company can demonstrate that it took all reasonable measures to prevent the breach. Showing that the company is compliant with a respected best practice standard, such as the ISO/IEC 27000 series or NIST Special Publication 800-53, will go a long way to protecting the company from both legal and nonlegal breach fallout. For smaller organizations without vast stores of sensitive data, this does not need to be a significant undertaking; there are off-the-shelf materials and audit criteria that can help guide assessment efforts. But regardless of size, organizations should consider conducting these assessments under the direction of counsel, to preserve privilege in case the assessment reveals any risk that later leads to a breach.

4. **Regularly train employees on data security**. While IT staff responsible for security operations should receive the most robust training, countless breaches have occurred through the actions of non-IT employees, from clicking on a virus in an email to losing a thumb drive containing sensitive information. Therefore, all employees should be trained on the company's data security policies when they first join the organization and then on a periodic basis thereafter.
5. **Incorporate data security into vendor management procedures**. Organizations are increasingly outsourcing data processing operations to service providers, so a key to maintaining an acceptable level of risk is conducting reasonable diligence of these providers and including security-specific terms into contracts.

NOTES

1. *See* Target, Data Breach FAQ, *https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ*.
2. Brian Krebs, "Email Attack on Vendor Set Up Breach at Target," *Krebs on Security*, Feb. 12, 2014, *http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target*.
3. Michael Riley et al., "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *Bloomberg Businessweek*, Mar. 13, 2014, *http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data*.
4. Privacy Rights Clearinghouse, Chronology of Data Breaches, *http://www.privacyrights.org/data-breach* (search for breaches classified as "Unintended disclosure" or "Hacking or malware" in 2013).
5. *See, e.g.*, Patco Const. Co., Inc. v. People's United Bank, 684 F.3d 197, 210–213 (1st Cir. 2012) (finding security procedures employed for Internet banking to be commercially unreasonable under the Uniform Commercial Code); Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2011 WL 2433383, at *14 (E.D. Mich. June 13, 2011) (concluding that bank was responsible for fraudulent wire transfers for failing to detect or stop aberrant transfers).
6. 15 U.S.C. § 45. The FTC also has authority to regulate data security under a few statutes regulating specific types of data, including consumer report information under the Fair Credit Reporting Act, children's personal information collected online under the Children's Online Privacy Protection Act, and nonpublic personal information held by financial institutions under the Gramm–Leach–Bliley Act. *See* 15 U.S.C. §§ 1681e(a), 6502(b)(1)(D), 6801–6809.
7. *See, e.g.*, Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 21 Mass. Code Regs. 17.00 (requiring entities that own or license certain sensitive consumer data of Massachusetts residents to document and implement a comprehensive information security program to protect that data, including the adoption of specific security measures); Nev. Rev. Stat. § 603A.215(2)(a) (prohibiting businesses from transferring sensitive consumer data over public networks unless the data is adequately encrypted); Justin J. Hakala, "Follow-On State Actions Based on the FTC's Enforcement of Section 5" (2008), available at *http://www.ftc.gov/sites/default/files/documents/public_comments/section-5-workshop-537633-00002/537633-00002.pdf*.
8. Two companies currently are facing charges that they violated the FTC Act by maintaining poor security practices, claiming that the FTC does not have the authority to regulate data security. While both cases are ongoing, in both of them there has been a decision that the FTC can bring actions based on a company's data security practices. *See* FTC v. Wyndham Worldwide Corp., No. 13-1887(ES), 2014 WL 1349019, at *9 (D.N.J. Apr. 7, 2014); In re LabMD, Inc., FTC File No. 102 3099, No. 9357, at 14 (F.T.C. Jan. 16, 2014), available at *http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf*. In every other publicly reported case, the investigated company has settled with the FTC.
9. *See* Press Release, FTC, "Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser" (Aug. 9, 2012), available at *http://ftc.gov/opa/2012/08/google.shtm*.
10. *See* Daniel J. Solove & Woodrow Hartzog, "The FTC and the New Common Law of Privacy," 114 *Columbia L.R.* 583, 622 (2014) ("The [FTC] orders are publicized with the intent that practitioners will rely on them, and practitioners do so.").
11. *See generally* Proposed Brief of *Amici Curiae* Chamber of Commerce of the United States of America, Retail Litigation Center, American Hotel & Lodging Association, and National Federation of Independent Business in Support of Defendants, FTC v. Wyndham Worldwide Corp., No. 2:13-cv-01887-ES-SCM, Dkt. 95-2 (D.N.J. filed May 3, 2013), available at *http://www.chamberlitigation.com/sites/default/files/cases/files/2013/U.S.%20Chamber%2C%20et%20al.%20Amicus%20Brief%20in%20Support%20of%20MTD%20--%20FTC%20v.%20Wyndham%20Worldwide%20Corp.%2C%20et%20al.%20%28U.S.%20Dist.%20Ct.%20for%20N.J.%29.pdf*.

12. *See also* Solove & Hartzog, *supra* n.10, at 650–655 (classifying list of data security practices generally considered inadequate by the FTC).
13. 15 U.S.C. § 45(n).
14. *See, e.g.*, Franklin's Budget Car Sales, Inc., FTC File No. 102 3094, No. C-4371, Compl. ¶ 10 (F.T.C. Oct. 3, 2012), available at *http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026franklinautomallcmpt.pdf* [hereinafter Franklin's Complaint] (action for breach of certain customer information which could "easily be misused to commit identity theft or fraud").
15. In re Sears Holdings Mgmt. Corp., FTC File No. 082 3099, No. C-4264, Compl. ¶ 13 (F.T.C. Aug. 31, 2009), available at *http://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf*. The FTC alleged this practice was deceptive because consumers were not given adequate disclosure of such a sensitive data collection practice. Other "over-collection" complaints have alleged unfairness as well. *See, e.g.*, In re Upromise, Inc., FTC File No. 102 3116, No. C-4351, Compl. ¶¶ 7, 20 (F.T.C. Mar. 27, 2012) [hereinafter Upromise Complaint].
16. In re Twitter, Inc., FTC File No. 092 3093, No. C-4316, Compl. ¶ 12 (F.T.C. Mar. 11, 2011), available at *http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf* [hereinafter Twitter Complaint]; *see also* United States v. RockYou, Inc., No. CV-12-1487, Compl. ¶ 14 (N.D. Cal. filed Mar. 26, 2012) [hereinafter RockYou Complaint] ("RockYou's practice of initially collecting email account passwords and storing them in clear text, even temporarily, created the risk of unauthorized access to such passwords and, therefore, to users' email accounts.").
17. *See, e.g.*, In re Eli Lilly & Co., 133 F.T.C. 763, 766-67 (2002) (complaint) (disclosure of consumers with particular drug subscription).
18. *E.g.*, FTC, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" 47 (2012), available at *http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf*.
19. In re Microsoft Corp., 134 F.T.C. 709, 711–712 (2002) (complaint) ("[R]espondent represented, expressly or by implication, that it maintained a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to protect the privacy and confidentiality of personal information obtained from or about consumers.... In truth and in fact, respondent did not maintain a high level of online security....").
20. Bret Cohen, "The Evolving Legal Framework Regulating Commercial Data Security Standards," 47 No. 1 *Md. B.J.* 31, 32–33 (2014).
21. *E.g.*, In re HTC Am. Inc., FTC File No. 122 3049, No C-4406, Compl. ¶ 21 (F.T.C. June 25, 2013), available at *http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf* [hereinafter HTC Complaint] ("HTC failed to employ reasonable and appropriate security practices in the design and customization of the software on its mobile devices. HTC's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.").
22. *See, e.g.*, Gerard M. Stegmaier & Wendell Bartnick, "Another Round in the Chamber: FTC Data Security Requirements and the Fair Notice Doctrine," 17 No. 5 *J. Internet L.* 17, 24–25 (2013) ("[T]he FTC's recent and historic notice methods in this area remain problematic under the fair notice doctrine, because they do not clearly distinguish the law from best practices or explain why legal requirements may apply in some cases and not others."); Michael D. Scott, "The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?," 60 *Admin. L. Rev.* 127, 165–171 (2008) ("No guidelines exist under which the FTC will act or refrain from acting if a data security breach occurs.").
23. *See, e.g.*, Solove & Hartzog, *supra* n.10 at 661–662; Stegmaier & Bartnick, *supra* n.22 at 23; United States v. ValueClick, Inc., No. CV08-01711MMM (RZx), Compl. ¶ 48 (C.D. Cal. filed Mar. 13, 2008) (referencing defendant's failure to encrypt sensitive consumer information "consistent with industry standards").
24. FTC, "Protecting Personal Information: A Guide for Business," available at *http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business* [hereinafter FTC Business Guide].
25. *Id.* at 10.
26. *E.g., id.* at 11; FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, Compl. ¶ 24(d) (D. Ariz. filed Aug. 9, 2012) (first amended complaint) (later transferred to D.N.J.), available at *http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf* [hereinafter Wyndham Complaint] ("Defendants ... failed to remedy known security vulnerabilities ..., thereby putting personal information held by Defendants ... at risk."); HTC Complaint ¶ 15 ("HTC could have detected its failure to deactivate the debug code in its CIQ Interface had it had adequate processes and tools in place for reviewing and testing the security of its software code."); Upromise Complaint ¶ 14(b) ("[R]espondent did not test the Targeting Tool before distributing it to consumers or monitor the Targeting Tool's operation thereafter to verify that the information it collected was consistent with respondent's policies."); In re MTS, Inc., 137 F.T.C. 444, 448 (2004) (complaint) [hereinafter MTS Complaint] ("Respondents created [a] vulnerability by failing to implement ... reasonable and appropriate procedures for writing and revising Web-application code. Among other things, Respondents failed 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."). Although Wyndham has not settled and is currently litigating this claim, s*ee supra* n.8, the FTC's allegations still reflect the data security standards it reads into Section 5.
27. *See, e.g.*, RockYou Complaint ¶ 16(c) ("Defendant failed to take reasonable measures to [protect user information] by, among other things: ... not protecting its website from such commonly known or reasonably foreseeable attacks from third parties attempting to obtain access to customer information stored in Defendant's databases. Defendant failed, for example, to address vulnerabilities in its system to web-based application attacks such as 'Structured Query Language' (SQL) injection attacks and 'Cross-Site Scripting' (XSS) attacks. During the relevant period, SQL injection and XSS attacks were well-known and well-publicized forms of hacking attacks, and solutions to prevent such attacks were readily-available and inexpensive.").
28. FTC Business Guide at 17; *see also* Open Web Application Security Project, OWASP Top 10 Project, *https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project*; SANS Institute, Critical Security Controls for Effective Cyber Defense, *http://www.sans.org/critical-security-controls*.
29. *E.g.*, FTC Business Guide at 10; Wyndham Complaint ¶ 24(i) (citing failures to monitor computer network for malware).
30. Danny Yadron, "Symantec Develops New Attack on Cyberhacking," *Wall St. J.*, May 4, 2014, available at *http://online.wsj.com/news/articles/SB10001424052702303417104579542140235850578*.
31. In re Dave & Buster's, Inc., 149 F.T.C. 1450, 1451 (2010) (complaint) [hereinafter Dave & Buster's Complaint].
32. FTC Business Guide at 16.
33. Franklin's Complaint ¶ 8(c).

34. *E.g.*, FTC Business Guide at 16; Dave & Buster's Complaint at 1451 ("[R]espondent … failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by employing an intrusion detection system and monitoring system logs."); In re TJX Cos., Inc., FTC File No. 072 3055, No. C-4227, Compl. ¶¶ 8(a)–(b) (F.T.C. July 29, 2008), available at *http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf* [hereinafter TJX Complaint] ("[R]espondent … failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by … following up on security warnings and intrusion alerts."); In re James B. Nutter & Co., FTC File No. 072 3108, No. C-4258, Compl. ¶ 6(4) (F.T.C. May 5, 2009), available at *http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090616nuttercmpt.pdf* ("[R]espondent … did not employ sufficient measures to prevent or detect unauthorized access to personal information on its computer network or to conduct security investigations, such as monitoring and controlling connections between the network and the internet or regularly reviewing activity on the network[.]").

35. *E.g.*, FTC Business Guide at 14; Wyndham Complaint ¶ 24(a) ("Defendants … failed to use readily available security measures to limit access between and among the Wyndham-branded hotels' property management systems, the Hotels and Resorts' corporate network, and the Interent, such as by employing firewalls[.]"); Dave & Buster's Complaint at 1451 ("[R]espondent … failed to use readily available security measures to limit access between in-store networks, such as by employing firewalls … .").

36. FTC Business Guide at 14.

37. *E.g.*, RockYou Complaint ¶ 16(c) ("Defendant failed to take reasonable measures to [protect its users' information] by … failing to segment its servers; once a hacker entered Defendant's network he or she was able to access all information on the network, including consumers' email addresses and RockYou passwords[.]"); Dave & Buster's Complaint at 1451 ("[R]espondent … failed to use readily available security measures to limit access between in-store networks, such as by … isolating the payment card system from the rest of the corporate network.").

38. *E.g.*, In re GMR Transcription Servs., Inc., FTC File No. 122 3095, Compl. ¶ 11 (F.T.C. Jan. 31, 2014), available at *http://www.ftc.gov/system/files/documents/cases/140203gmrcmpt.pdf* [hereinafter GMR Complaint] (alleging that company failed to require contractors "to adopt and implement security measures, such as installing anti-virus applications, or confirm that they had done so," and also failed to "adequately verify" that a service provider would secure sensitive consumer data by not conducting diligence about the provider's security practices and not requiring certain security-related provisions in the contract); In re ACRAnet, Inc., FTC File No. 092 3088, No. C-4311, Compl. ¶¶ 7(b)–(c) (F.T.C. Aug. 17, 2011), available at *http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110809acranetcmpt.pdf*; ("[R]espondent failed to … assess the risks of allowing end users with unverified or inadequate security to access consumer reports through ACRAnet's portal [and] implement reasonable steps to address these risks by, for example, evaluating the security of end user's [sic] computer networks, requiring appropriate information security measures, and training end user clients[.]").

39. Wyndham Complaint ¶¶ 24(c)–(d), (j).

40. *E.g.*, FTC Business Guide at 10, 15; TJX Complaint ¶¶ 8(a), (b) ("[R]espondent: (a) created an unnecessary risk to personal information by storing it on, and transmitting it between and within, in-store and corporate networks in clear text; [and] (b) did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to in-store networks without authorization[.]").

41. *See, e.g.*, FTC Business Guide at 10–11, 13, 15; GMR Complaint ¶ 12 (FTP).

42. *E.g.*, FTC Business Guide at 10; In re Fandango, LLC, FTC File No. 132 3089, Compl. ¶ 15 (F.T.C. Mar. 28, 2014), available at *http://www.ftc.gov/system/files/documents/cases/140328fandangocmpt.pdf* (finding mobile application failed to provide reasonable and appropriate security in part because it failed to validate SSL certificates, overriding the defaults provided by the operating system).

43. FTC Business Guide at 10.

44. *See, e.g.*, Wyndham Complaint ¶ 24(b) (finding storage of payment card information in clear readable text to be "unreasonable" when other vulnerabilities allowed hackers to access the data); RockYou Complaint ¶ 16(b) (finding storage of user passwords in clear text "unreasonable" where a hacker accessed the unencrypted data using SQL injection and cross-site scripting attacks).

45. *E.g.*, In re LabMD, Inc., FTC File No. 102 3099, No. 9357, Compl. ¶ 10(g) (F.T.C. Aug. 28, 2013), available at *http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf* [hereinafter LabMD Complaint ¶¶ 13-16] ("[R]espondent … did not use appropriate measures to prevent employees from installing on computers applications or materials that were not needed to perform their jobs[, and thus] did not detect the installation or use of an unauthorized file sharing application on its networks."); Franklin's Complaint ¶¶ 8–11 (alleging that company's alleged failure to adopt policies to prevent employees from downloading peer-to-peer software that exposed sensitive data was an unreasonable practice). Although LabMD has not settled and is currently litigating this claim, s*ee supra* n.8, the FTC's allegations still reflect the data security standards it reads into Section 5.

46. In re Lookout Servs., Inc., 151 F.T.C. 532, 535–36 (2011) (complaint) [hereinafter Lookout Complaint].

47. MTS Complaint ¶¶ 8–9.

48. *See, e.g.*, LabMD Complaint; Wyndham Complaint ¶¶ 24(e)–(f); Lookout Complaint at 534–535; Twitter Complaint ¶ 11; In re Reed Elsevier Inc., FTC File No. 052 3094, No. C-4226, Compl. ¶ 10(a)–(g) (F.T.C. July 29, 2008), available at *http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reedcomplaint.pdf*; FTC Business Guide at 12.

49. *See* LabMD Complaint ¶ 10(e).

50. *See generally* Kenneth A. Bamberger & Deirdre K. Mulligan, "Privacy on the Books and on the Ground," 63 *Stan. L. Rev.* 247 (2011).