Washington Legal Foundation
Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

Critical Legal Issues: WORKING PAPER SERIES

DATA SECURITY BEST PRACTICES DERIVED FROM FTC § 5 ENFORCEMENT ACTIONS

Kurt Wimmer, Ashden Fein,
Catlin M. Meade & Andrew Vaden
Covington & Burling LLP

Foreword by David A. Heiner
Vice President & Deputy General Counsel
Microsoft Corporation

Washington Legal Foundation
Critical Legal Issues WORKING PAPER Series

Number 199
January 2017

TABLE OF CONTENTS

ABOUT WLF'S LEGAL STUDIES DIVISION ii

ABOUT THE AUTHORS iii

FOREWORD iv

INTRODUCTION 1

FUNDAMENTALS OF FTC'S § 5 AUTHORITY 2

DATA SECURITY BEST PRACTICES DERIVED FROM FTC ENFORCEMENT ACTIONS 4

A. Standard 1: Limit the Collection, Retention, and Use of Sensitive Data 7

B. Standard 2: Restrict Access to Sensitive Data 9

C. Standard 3: Implement Robust Authentication Procedures 11

D. Standard 4: Store and Transmit Sensitive Information Securely 13

E. Standard 5: Implement Procedures to Identify and Address Vulnerabilities 15

F. Standard 6: Develop and Test New Products and Services with Privacy and Security in Mind 18

G. Standard 7: Require Service Providers to Implement Appropriate Security Measures 20

H. Standard 8: Properly Secure Documents, Media, and Devices 21

CONCLUSION 22

ABOUT WLF'S LEGAL STUDIES DIVISION

Washington Legal Foundation (WLF) established our Legal Studies division in 1986 to address cutting-edge legal issues through producing and distributing substantive, credible publications designed to educate and inform judges, policy makers, the media, and other key legal audiences.

Washington is full of policy centers of one stripe or another. From the outset, WLF's Legal Studies division adopted a unique approach to set itself apart from other organizations in several ways.

First, Legal Studies focuses on legal matters as they relate to sustaining and advancing economic liberty. The articles we solicit tackle legal policy questions related to principles of free enterprise, individual and business civil liberties, limited government, and the Rule of Law.

Second, WLF's publications target a highly select legal policy-making audience. We aggressively market our publications to federal and state judges and their clerks; Members of Congress and their legal staff; Executive Branch attorneys and regulators; business leaders and corporate general counsel; law professors; influential legal journalists, such as the Supreme Court press; and major media commentators.

Third, Legal Studies operates as a virtual legal think tank, allowing us to provide expert analysis of emerging issues. Whereas WLF's in-house appellate attorneys draft the overwhelming majority of our briefs, Legal Studies possesses the flexibility to enlist and the credibility to attract authors with the necessary background to bring expert perspective to the articles they write. Our authors include senior partners in major law firms, law professors, sitting federal judges, other federal appointees, and elected officials.

But perhaps the greatest key to success for WLF's Legal Studies project is the timely production of a wide variety of readily intelligible but penetrating commentaries with practical application and a distinctly commonsense viewpoint rarely found in academic law reviews or specialized legal trade journals. Our eight publication formats are the concise COUNSEL'S ADVISORY, topical LEGAL OPINION LETTER, provocative LEGAL BACKGROUNDER, in-depth WORKING PAPER, useful and practical CONTEMPORARY LEGAL NOTE, informal CONVERSATIONS WITH, balanced ON THE MERITS, and comprehensive MONOGRAPH.

WLF's LEGAL OPINION LETTERS and LEGAL BACKGROUNDERS appear on the LEXIS/NEXIS® online information service under the filename "WLF," and every WLF publication since 2002 appears on our website at www.wlf.org.

To receive information about previous WLF publications, or to obtain permission to republish this publication, please contact Glenn Lammi, Chief Counsel, Legal Studies, Washington Legal Foundation, 2009 Massachusetts Avenue, NW, Washington, D.C. 20036, (202) 588-0302, glammi@wlf.org.

ABOUT THE AUTHORS

Kurt Wimmer is a Partner at Covington & Burling LLP and chairs the firm's Data Privacy and Cybersecurity practice. He represents clients on privacy, cybersecurity, and technology law issues. He was past chair of the Privacy and Information Security Committee of the Antitrust Section of the American Bar Association. Mr. Wimmer is the former general counsel of Gannett Corp.

Ashden Fein is an Associate at Covington & Burling LLP. He represents clients on cybersecurity and national security matters. He counsels clients on preparing for and responding to cyber-based attacks on their networks, assessing their cybersecurity controls and practices for data protection, developing and implementing information security programs, and complying with federal and state regulatory requirements. Prior to joining Covington & Burling, he served for 13 years in the United States Army as an intelligence officer and a military prosecutor.

Catlin Meade is an Associate at Covington & Burling LLP. She represents clients across a broad range of cybersecurity matters, including compliance with cybersecurity and data breach regulations.

Andrew Vaden is an Associate at Covington & Burling LLP. He represents clients on privacy and cybersecurity matters. He clerked for a judge on the U.S. Court of Appeals for the Fifth Circuit. Prior to law school, he served for eight years as a Foreign Service Officer with the U.S. Department of State.

The authors acknowledge the significant involvement of Covington & Burling LLP Of Counsel **Richard A. Hertling** in the development and review of this WORKING PAPER.

FOREWORD

By
David A. Heiner[1]
Microsoft Corporation

We are awash in data. The rapidly-accelerating digitization of seemingly everything and the rapidly declining cost of data storage means that governments, businesses, and others have access to unprecedented volumes of data. Recent advances in data-analytics techniques are enabling patterns to be discerned in huge data sets. These patterns, often quite subtle, but nonetheless real, are enabling organizations of all types to derive important insights and make predictions about the world in which we live. And data—lots and lots of data—is the most essential ingredient in the rapid advances in artificial intelligence over the past few years. Artificial intelligence systems learn from "experience." For a computer, experience comes in the form of data.

The promise of artificial intelligence (and data analytics generally) is transforming every aspect of Microsoft's business, where I've worked as a lawyer for more than twenty years. Microsoft is investing heavily in building artificial intelligence techniques into a wide range of its products and—critically—making these techniques available to software developers and organizations of all sizes so that everyone can benefit from them. Cortana, the "personal assistant" recently introduced by Microsoft, provides an early glimpse of what will be possible. Already "she" can offer reminders, track packages and flights, suggest restaurants and answer a wide range of questions. Soon she will be able to schedule

[1]David A. Heiner is Vice President and Deputy General Counsel of the Regulatory Affairs team at Microsoft Corporation.

meetings, or even book an entire vacation. That is made possible in part by the millions of questions people have already posed, and their reactions to her answers—data. Data is key, too, to Microsoft Translator, which can translate speech from one language to another, in real-time, and is getting better every day as more people use it. Amazon, Google, IBM and others are introducing their own innovations, all made possible by access to vast troves of data.

That may be data about the environment, the economy, industrial processes—or people. Seemingly overnight, privacy concerns have become paramount. And the stakes are high: technological advances that can improve health care, education, economic efficiency, and more are dependent on the collection and use of personal data, and the very existence of all that data raises the specter of a "surveillance state" where the government, or other organizations, know far more about each of us than ever before. Civil rights advocates fear that "big data" may be used, intentionally or unintentionally, in ways that discriminate against vulnerable populations. And well-publicized data breaches at big-name companies have consumers on high alert.

In this environment, every organization that wants to work with personal data needs to be responsible and accountable. But this is no easy task. One of the complications is the variety of data protection laws around the world. The European Union has taken a step toward rationalizing this with the recently passed General Data Protection Regulation, which provides a comprehensive framework applicable across Europe. In the United States, privacy law is sectoral, driven by a combination of national and state laws applicable to specific industries. Microsoft has long favored the adoption of comprehensive U.S. privacy legislation

to address the uncertainty businesses faces when confronted with varying U.S. privacy requirements.

For now organizations working with personal data must tread carefully, developing a comprehensive approach that can account for the patchwork of U.S. legal requirements. And for all of them, a primary consideration is the Federal Trade Commission's (FTC) 200-plus privacy and security-related enforcement actions (which includes the approximately 60 actions related to data security on which this WORKING PAPER focuses). FTC is the largest of the US agencies focused on consumer protection, and for more than fifteen years, it's been the leader in protecting privacy and data security through its general Section 5 authority, in addition to enforcing a handful of specific privacy laws. Recently, it also took on a new role as the key enforcer of the EU-US Privacy Shield, which is fundamental to enabling data to flow between Europe and the United States.

Since bringing its first privacy-focused action against GeoCities in 1998, FTC has evolved into the broadest and most powerful data protection agency in the US. Federal courts have endorsed FTC's fact-based approach, but the breadth and depth of issues the agency has evaluated is vast. Few organizations have the time or resources to take a deep dive into the many nuances that inevitably flow from the FTC's "case-by-case" regulatory approach. This WLF WORKING PAPER will help to rectify that. The authors' thorough analysis of what is sometimes called FTC's "common law" of privacy provides a cogent explanation of this multi-faceted area of FTC law. I wish Microsoft had such a resource back in 2002, when it entered into its own privacy-related consent decree with FTC—but better late than never!

I have no doubt that this comprehensive study of FTC's § 5 enforcement actions will

be a great aid for any U.S. company dealing with personal data. The WORKING PAPER carefully traces the history of FTC's authority, and neatly distills the key takeaways into fundamental principles that companies can use as a compass to help navigate through this complex area of law. With FTC's work and this paper's explanation of it as a baseline, we can all work toward finding the right ways to enable technological advances in the years ahead while preserving privacy.

DATA SECURITY BEST PRACTICES DERIVED FROM FTC § 5 ENFORCEMENT ACTIONS

INTRODUCTION

In the United States, there is no general federal privacy or data security law. Instead, a number of federal and state agencies have independently established their own sector-specific controls and requirements through a thicket of regulations, enforcement actions, and best-practice guidance documents. The Federal Trade Commission is one of the more forward-leaning agencies focusing on protecting consumers and the privacy of their data. Specifically, FTC has exercised its enforcement authority under § 5 of the Federal Trade Commission Act (FTC Act) to prohibit "unfair or deceptive acts or practices" in the area of *consumer* data security.[1] Since 2002, FTC has used this authority to protect consumers' sensitive information from breaches or inadvertent disclosures and has undertaken approximately 60 enforcement actions against corporations and individuals on data-security matters to date.

FTC does not define or prescribe data privacy and security standards via regulation. It relies instead on a combination of its enforcement activities and guidance to the business community to establish what trade practices are "deceptive" or "unfair." Courts have endorsed this case-by-case approach to establishing standards, reasoning that Congress explicitly considered and rejected the idea that prohibited trade practices could be

[1] 5 U.S.C. § 45.

comprehensively enumerated to avoid ambiguity.[2] Although deriving concrete standards from FTC's numerous and evolving enforcement decisions is not a simple matter, those subject to FTC's jurisdiction are nonetheless charged with notice of the applicable standards.

This WORKING PAPER traces the contours of FTC's authority in this vital area and examines all relevant enforcement actions before both the agency and the federal courts. Careful consideration of FTC's complaints and settlements yields important insights into how the Commission wields its authority and what security standards it expects companies under its purview to meet.

FUNDAMENTALS OF FTC'S § 5 AUTHORITY

Section 5 of the FTC Act directs the Commission to prevent companies from using "unfair or deceptive acts or practices in or affecting commerce." FTC's jurisdiction, however, does not extend to common carriers, banks and savings and loan institutions, certain air carriers, or certain entities subject to the Packers and Stockyards Act of 1921.[3]

The meanings of "unfair" and "deceptive" have been clarified by statute, caselaw, and FTC's exercise of its enforcement authority. To constitute an unfair act or practice, the conduct in question must cause substantial consumer injury, must not be outweighed by any countervailing benefits to consumers or competition, and must be an injury that consumers could not reasonably have avoided.[4] Whether an act or practice is deceptive depends on

[2] *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3d Cir. 2015); *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972).

[3] 15 U.S.C. § 45(a)(2).

[4] 15 U.S.C. § 45(n).

whether it contains a misrepresentation or omission that is likely to mislead consumers, who act reasonably under the circumstances, to their detriment. The misrepresentation may be either express or implied, but it must be material from the perspective of a reasonable consumer—that is, it must be likely to affect the choice or conduct of a reasonable member of the targeted group of consumers with respect to a product or service.[5] In practice, FTC often charges that unreasonable data-security practices were both unfair and deceptive because they resulted in consumer injury and were contrary to various representations in the respondent's privacy policy, website, or advertising.

Most proceedings begin when FTC issues an administrative complaint. If, after an opportunity to be heard, the respondent is found to have committed a deceptive or unfair trade practice, the Commission may order it to cease and desist from that practice. Any party subject to such an order may file a petition for review in a federal court of appeals.[6] In addition, the Commission can directly proceed to federal court by filing a complaint. In such cases, the Commission must prove that the defendant acted with actual or constructive knowledge that the act was unfair or deceptive.[7]

Even when the § 5 criteria are met in a matter involving privacy and data security, the Commission may decline to file a complaint based on a number of factors, including "the extent to which the risk was reasonably foreseeable at the time of compromise," "the benefits relative to the costs of protecting against the risk," the company's "overall data

[5] *Fanning v. FTC*, 821 F.3d 164, 170 (1st Cir. 2016).

[6] 15 U.S.C. § 45(b), (c), (l).

[7] 15 U.S.C. § 45(m)(1).

security practices," and the speed of the company's response to the incident.[8]

Although some companies do avail themselves of the adversarial process to defend against a complaint, FTC enforcement actions usually lead to a settlement with FTC in which the parties agree to the entry of a consent order. These consent orders often provide for broad injunctive relief, including the implementation of company-wide compliance programs, third-party and FTC audits for periods as long as 20 years, and other requirements that affect the company's data-processing practices. Once an order enters into force, the government may bring a civil action for noncompliance with its provisions.

Noncompliance with a consent order can come at a heavy price. Last year, Lifelock paid $100 million to settle FTC charges that it violated the terms of such an order by failing to maintain a comprehensive information security program, engaging in deceptive advertising relating to its protection of customers' sensitive data, and neglecting to adhere to recordkeeping requirements set out in the order.[9]

DATA SECURITY BEST PRACTICES DERIVED FROM FTC ENFORCEMENT ACTIVITIES

"[T]he Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing

[8]FTC Letter to Dollar Tree Stores, Inc. (June 5, 2007), https://www.ftc.gov/sites/default/files/documents/closing_letters/dollar-tree-stores-inc./070605doltree.pdf; *see also* FTC Letter to *Morgan Stanley Smith Barney LLC* (Aug. 10, 2015), https://www.ftc.gov/system/files/documents/closing_letters/nid/150810morganstanleycltr.pdf; FTC Letter to Lime Wire LLC (Aug. 19, 2010), https://www.ftc.gov/sites/default/files/documents/closing_letters/lime-wire-llc/100919limewireletter.pdf.

[9]*FTC v. Lifelock Inc.*, 2016 WL 692048 (D. Ariz. Jan. 4, 2016); FTC, *LifeLock to Pay $100 Million to Consumers to Settle FTC Charges it Violated 2010 Order* (Dec. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated.

risks."[10] It is most likely to fault companies that neglect to use "readily available, low-cost measures" to address data security vulnerabilities.[11] FTC also focuses on whether a company's data-security practices comport with what the company publicly claims to be doing with consumers' data in its privacy policy or in advertising.

The most conclusive sources of guidance on what constitutes an unfair or deceptive data-security practice are FTC's enforcement activities, including administrative complaints, suits in federal court, and consent agreements between FTC and various respondents. FTC has also published a variety of informal guidance for businesses, apprising them of their responsibilities and detailing how FTC's enforcement actions are consonant with other federal guidance such as the National Institute of Standards and Technology's Cybersecurity Framework.[12] Although a determination that particular data-security practices are so lax as to be unfair is necessarily a fact-intensive determination, an analysis of these sources establishes a number of data privacy and security standards that FTC expects those subject to its jurisdiction to follow.

As industry standards evolve, FTC assumes companies are aware of best practices and widely known vulnerabilities. As the Commission has emphasized, "data security is an

---

[10] *In re LabMD, Inc.*, No. 9357 (FTC July 29, 2016).

[11] Complaint at 5 (¶ 17), *In re Compete, Inc.*, No. C-4384 (FTC Feb. 25, 2013).

[12] *See, e.g.*, FTC, *The NIST Cybersecurity Framework and the FTC* (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc; FTC, *Start with Security, A Guide for Business: Lessons Learned from FTC Cases* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; FTC, *Protecting Consumer Privacy in an Era of Rapid Change* (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

ongoing process, and ... as risks, technologies, and circumstances change over time, companies must adjust their information security programs accordingly."[13] For example, at least one complaint has noted that free tools exist to monitor "security vulnerability reports from third-party researchers, academics, [and] other members of the public," and cited the respondent for its failure to monitor and respond to such reports.[14] As outlined below, the Commission has even reversed itself on one issue in light of developing research: although it used to cite companies for failure to require that passwords be changed periodically, it has now acknowledged that the case for such mandatory changes is weak.

The remainder of this WORKING PAPER outlines the following eight overarching standards derived from FTC enforcement actions that generally apply to all consumer-facing companies:

- limit the collection, retention, and use of sensitive data;
- restrict access to sensitive data;
- implement robust authentication procedures;
- store and transmit sensitive information securely;
- implement procedures to identify and address vulnerabilities;
- develop and test new products and services with privacy and security in mind;
- require service providers to implement appropriate security measures; and
- properly secure documents, media, and devices.

This list is not exhaustive and does not include enforcement actions taken by FTC under the Gramm-Leach-Bliley Act Safeguards Rule.[15] Rather, the list highlights standards that FTC has

[13] FTC Letter to Monster Worldwide, Inc. 2 (Mar. 6, 2008), https://www.ftc.gov/sites/default/files/documents/closing_letters/monster-worldwide-inc./monsterworldwide.pdf.

[14] Complaint at 4 (¶ 8), *In re TRENDNet, Inc.*, No. C-4426 (FTC Jan. 16, 2014); *see also* Complaint at 11-12 (¶ 42), *United States v. ValueClick, Inc.*, No. CV08-1711 (C.D. Cal. Mar. 17, 2008) (discussing sites' vulnerability to "commonly known or reasonably foreseeable" attacks, including SQL injection attacks).

[15] 16 C.F.R. Part 314.

imposed with some frequency and that FTC expects companies within its jurisdiction to follow.

A. Standard 1: Limit the Collection, Retention, and Use of Sensitive Data

FTC has repeatedly stressed that companies should collect and retain only as much sensitive information as is needed. Collecting more information than it needs—or keeping it longer than necessary—makes a company a more appealing target for criminals and risks that any breach will result in additional, avoidable damage. FTC enforcement actions espousing this standard have also addressed the situation in which a consumer's sensitive personal information is legitimately collected and retained, but the company unnecessarily exposed that information to greater risk of unauthorized disclosure or theft. For example, FTC has filed complaints against companies that collect, retain, or use data in a manner contrary to the stated purpose in their privacy policies by sharing the information with potential customers or using the information in training exercises.

1. *Only Collect Information that Is Necessary*

- In 2012, FTC brought a complaint in federal district court against **RockYou**, a company whose website allowed users to develop content for posting on social networking sites. To register for the site, users were required to provide their email address *and email password*. FTC—alleging that RockYou's practice of collecting email account passwords created the unnecessary risk of unauthorized access to users' email accounts—charged that this practice was contrary to the representations in its privacy policy that it would employ reasonable safeguards to protect its users' information.[16] Although the complaint in *RockYou* casts this practice in terms of deception, the same logic would support an unfairness claim.

- FTC pursued **DesignerWare**, the developer and licensor of software for rent-to-own stores to install in rented computers which could disable the

[16]Complaint at 4-5 (¶¶ 14, 16), *United States v. RockYou, Inc.*, No. 12-CV-1487 (N.D. Cal. Mar. 28, 2012).

device when the renter stopped making payments or otherwise breached the agreement. The software could also be used to monitor the users (including logging keystrokes, taking pictures with the computer's webcam, and causing fake registration popups to collect information) and track the computer's physical location. None of this information was necessary to the rent-to-own store, and the renters were not told that this software was installed on the computers. As a result, FTC found that DesignerWare provided the means and instrumentalities for the commission of unfair acts and practices and caused substantial injury to consumers that were not outweighed by countervailing benefits to consumers or competition.[17] Similarly, FTC found **Snapchat** committed violations of § 5 by collecting geolocation and contacts information despite statements it posted in its privacy policy suggesting that type of information was not collected.[18]

2. *Only Retain Information for as Long as Necessary*

- In ***BJ's Wholesale Club***, the company's misconfigured wireless access points allowed at least one savvy user to anonymously access stored data on the stores' network. Damages from the breach were amplified by the fact that the company stored customers' credit card information for up to 30 days after it was used. Noting that BJ's had no business need for the information, FTC faulted the company for creating unnecessary risks by retaining sensitive data for an extended period and filed an unfair practices charge against the company based, in part, on that conduct.[19] The Commission took similar actions against **CardSystems Solutions, Inc**., and **Life is Good, Inc**.[20]

3. *Only Use Customer Information for a Proper Purpose*

- FTC charged **Accretive Health**, an accounting and billing service provider for hospitals, with an unfair trade practice because it "created unnecessary risks of unauthorized access or theft of personal information" in various ways, including, for example by using consumers' personal information in

[17] *In re DesignerWare, LLC*, No. C-4390 (FTC Apr. 11, 2013).

[18] *See* Complaint 5-7 (¶¶ 20-31), *In re Snapchat, Inc.*, No. C-4501 (FTC Dec. 23, 2014).

[19] Complaint at 2 (¶ 7), *In re BJ's Wholesale Club, Inc.*, No. C-4148 (FTC Sep. 20, 2005).

[20] Complaint at 2 (¶ 5-6), *In re CardSystems Solutions, Inc.*, No. C-4168 (FTC Sept. 5, 2006) (storing card authorization responses for up to 30 days created unnecessary risk to the information); Complaint at 2 (¶ 8), *In re Life is Good, Inc.*, No. C-4218 (FTC Apr. 16, 2008) (storing consumer information indefinitely on its network in clear, readable text was unnecessary risk).

employee training sessions without ensuring that the information was removed from employees' computers following the training.[21]

- Similarly, nutritional supplement manufacturers **foru International** and **GeneLink** were the target of an unfair practice complaint by FTC partially due to their unnecessarily broad use of personal information. FTC alleged that the companies, among other things, put consumer data at unnecessary risk by: keeping sensitive personal information in clear text, providing all employees with full access to consumers' personal information regardless of business need, and providing service providers with access to consumers' complete personal information.[22]

- In two cases, ***Cornerstone*** and ***Bayview***, companies that were seeking to sell consumer-debt portfolios, posted Microsoft Excel files for prospective buyers that contained unnecessarily large amounts of consumer personally identifiable information. FTC clarified that some sharing of sensitive data in these cases is appropriate, but it also criticized sellers who do not "keep it to a minimum."[23]

- Two other cases, ***ChoicePoint*** and ***Rental Research Services***, illustrate the importance of confirming the bona fides of potential purchasers of sensitive data. The companies in these cases failed to take reasonable steps to verify their purchasers' identities, and allegedly gave sensitive consumer information directly to identity thieves.[24]

B. Standard 2: Restrict Access to Sensitive Data

FTC has often cited companies that fail to restrict access to sensitive data and systems. Although cases in this category concern technical controls on administrative accounts and remote access, they are animated by a common theme: access to sensitive

[21]Complaint at 2 (¶ 7), *Accretive Health, Inc.*, No. C-4432 (FTC Feb. 5, 2014).

[22]Complaint at 13 (¶ 29), *In re foru Int'l Corp.*, No. C-4457 (FTC May 8, 2014); Complaint at 13 (¶ 29), *In re GeneLink, Inc.*, No. C-4456 (FTC May 8, 2014).

[23]*See FTC v. Cornerstone & Co*., No. 1-14-CV-1479-RC (D.D.C. Apr. 21, 2015); *FTC v. Bayview Solutions, LLC*, No. 1-14-CV-1830-RC (D.D.C. Apr. 21, 2015); *see also* FTC, *Buying or Selling Debts? Steps for Keeping Data Secure* 2, https://www.ftc.gov/system/files/documents/plain-language/pdf-0202_buying-selling-debt.pdf.

[24]*United States v. ChoicePoint, Inc.*, No. 1:06-CV-198 (N.D. Ga. Feb. 15, 2006); *United States v. Rental Research Servs., Inc.*, No. 09-cv-524 (D. Minn. Mar. 5, 2009).

information should be permitted only when a business need is present. As with the above standard, FTC will often compare statements in a company's privacy policy with the data security being deployed. As a result, when a company promises to protect a consumer's information, FTC will use that promise of protection to issue a complaint against a company it deems to have lax data-security practices.

1. *Deploy the Principle of Least Privilege*

- FTC alleged that **Twitter** had provided "almost all" of its employees with administrative control of the system. As a result, almost any employee could "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." The company thus failed to "prevent unauthorized access to nonpublic user information and honor the privacy choices exercised by its users in designating certain tweets as nonpublic."[25]

2. *Deploy Network Security to Protect Sensitive Data*

- Hackers, who had obtained access to two hotel computers, were able to parlay their access into the broader property management system of **Wyndham Worldwide**. The FTC complaint that followed criticized the company for "fail[ing] 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 internet, such as by employing firewalls."[26]

- FTC found that **TJX**, the owner of off-price retail stores, had, among other things, failed to use readily available security measures to limit unauthorized wireless access to its in-store networks. Additionally, because personal data collected from consumers was stored and transmitted between stores and the corporate network in an unencrypted form, intruders were able to connect to the network and download personal information in clear text.[27]

---

[25]Complaint at 2-3 (¶¶ 7, 11), *In re Twitter, Inc.*, No. C-4316 (FTC Mar. 2, 2011).

[26]Complaint at 10 (¶ 24), *FTC v. Wyndham Worldwide Corp.*, No. 2:13-CV-1887-ES-JAD (D.N.J. Dec. 11, 2015).

[27]Complaint at 2 (¶ 8), *In re TJX Companies, Inc.*, No. C-4227 (FTC July 29, 2008).

3. *Ensure Individuals with Remote Access Have Adequate Security*

- The most basic conclusion of the cases involving endpoint security is that users permitted remote access to a network must have adequate antivirus protection. In ***Lifelock***, FTC supported a deceptive practices case against the company by noting that it "[f]ailed to employ sufficient measures to detect and prevent unauthorized access to the corporate network," including by neglecting to "install[] antivirus or anti-spyware programs on computers used by employees to remotely access the network."[28]

- The same is true when third parties, such as service providers or customers, are permitted access to a network used to process sensitive information. FTC filed a complaint against **Premier Capital Lending** after an employee created a remote login account for a business associate to access a credit reporting agency portal. A hacker later gained access to the associate's computer and used the credentials to request credit reports on hundreds of individuals without authorization. FTC faulted the company for failing to "evaluat[e] the security of the third party's computer network [or] tak[e] steps to ensure that appropriate data security measures were present."[29] Similarly, FTC filed a complaint against **SettlementOne Credit Corporation** for, among other things, allowing end users with unverified or inadequate security to access consumer reports through its online portal.[30] Similar actions were taken against **ACRAnet, Inc.**, and **Fajilan and Associates, Inc**.[31]

C. Standard 3: Implement Robust Authentication Procedures

Strict controls are necessary to ensure that access privileges for sensitive data are not misused. This includes: requiring complex passwords, storing passwords securely, suspending or disabling accounts after a set number of login attempts, and ensuring authentication procedures cannot be easily bypassed.

---

[28]Complaint at 10 (¶ 20), *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MHM (D. Ariz. Mar. 9, 2010).

[29]Complaint at 4 (¶ 14), *In re Premier Capital Lending*, No. C-4241 (FTC Dec. 10, 2008).

[30]Complaint at 2 (¶ 8(b)), *In re SettlementOne Credit Corp.*, No. C-4330 (FTC Aug. 17, 2011).

[31]Complaint at 2-3 (¶¶ 7-9), *In re ACRAnet, Inc.*, No. C-4331 (FTC Aug. 17, 2011); Complaint at 2-3 (¶¶ 7-9), *In re Fajilan and Associates, Inc.*, No. C-4332 (FTC Aug. 17, 2011).

1. *Require Complex and Unique Passwords and Store Passwords Securely*

- In the *Twitter* action discussed above, FTC also noted that the nascent company failed to "establish or enforce policies sufficient to make administrative passwords hard to guess, including policies that ... prohibit the use of common dictionary words as administrative passwords."[32] FTC also faulted Twitter for both not mandating that administrator passwords be unique—such as requiring employees to have unique passwords for the Twitter network and third-party accounts—and not encrypting stored passwords.

2. *Suspend or Disable Accounts after a Set Number of Failed Login Attempts*

- FTC filed a complaint against **Lookout Services**, which contracted with employers to confirm their new employees' I-9 information. The Commission alleged that the company "failed to suspend user credentials after a certain number of unsuccessful login attempts."[33]

- FTC also filed a complaint against **Reed Elsevier** for, among other things, "permitt[ing] the sharing of user credentials among a customer's multiple users" and "fail[ing] to require periodic changes of user credentials ... for customers with access to sensitive nonpublic information."[34]

3. *Ensure Authentication Measures Cannot Be Bypassed*

- In the *Lookout Services* case discussed above, FTC also identified another common cyber-related risk exploited by hackers: system authentication being entirely bypassed if the location of protected information-technology resources can be surmised from using standard naming conventions within the network. Attackers exploited this vulnerability in the course of their breach of Lookout Services' database, and FTC cited this "widely-known security flaw[]" in its § 5 complaint.[35]

---

[32]Complaint at 4 (¶ 11), *In re Twitter, Inc.*, No. C-4316 (FTC Mar. 2, 2011); *see* FTC, *Start with Security, A Guide for Business: Lessons Learned from FTC Cases* 8 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[33]Complaint at 2-3 (¶¶ 7-10), *In re Lookout Servs., Inc.*, No. C-4326 (FTC June 15, 2011). *See also* Complaint at 4 (¶ 11), *In re Twitter, Inc.*, No. C-4316 (FTC Mar. 2, 2011) (failure to suspend or disable accounts after multiple failed login attempts to protect against automated attacks).

[34]Complaint at 3 (¶ 10), *In re Reed Elsevier Inc.*, No. C-4226 (FTC June 1, 2009).

[35]Complaint at 2 (¶ 7), *In re Lookout Servs., Inc.*, No. C-4326 (FTC June 15, 2011).

- An authentication bypass vulnerability was also at issue in ***ASUSTeK***, a router manufacturer. The company touted a "secure cloud" service powered by its routers that allowed users to securely store files and selectively share them. Due to a programming error, however, an attacker with knowledge of the router's internet protocol address could bypass the authentication screen by "simply entering a specific URL in a web browser."[36]

4. *Require Regular Password Changes*

- Some FTC complaints—such as *Lookout Services* and *Reed Elsevier*—have faulted respondents for "fail[ing] to require periodic changes of user credentials, such as every 90 days, for customers and employees with access to sensitive personal information."[37] As later FTC guidance has acknowledged, however, "there is a lot of evidence to suggest that users who are required to change their passwords frequently select weaker passwords to begin with, and then change them in predictable ways that attackers can guess easily."[38] Given the state of research in this area, it seems less likely that FTC would consider a failure to expire passwords periodically a significant factor in a future § 5 investigation.

D. Standard 4: Store and Transmit Sensitive Information Securely

Although it is important that companies securely collect sensitive information from consumers, the obligation to secure the information applies with the same force to storing and transmitting that information. A number of FTC complaints reinforce the rule that sensitive data should be encrypted during storage and transmission, including the complaint against **DSW**.[39] The Commission has emphasized the accessibility of publicly-available free

[36]Complaint at 2-3 (¶ 9-10), *In re ASUSTeK Computer Inc.*, No. C-4587 (FTC July 18, 2016).

[37]Complaint at 2 (¶ 7), *In re Lookout Servs., Inc.*, No. C-4326 (FTC June 15, 2011); *see also* Complaint at 3 (¶ 10), *In re Reed Elsevier Inc.*, No. C-4226 (FTC June 1, 2009).

[38]Lorrie Cranor, *Time to Rethink Mandatory Password Changes*, FTC (Mar. 2, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes.

[39]*See, e.g.*, Complaint at 2 (¶ 7), *In re DSW, Inc.*, No. C-4157 (FTC Mar. 7, 2006).

software to encrypt transmissions of sensitive data "since at least 2008[.]"[40] As a result, FTC has brought a number of actions against companies who have failed to implement at least reasonable and low-cost security solutions when storing or transmitting consumers' sensitive information.

1. *Protect Information in the Manner Promised to Consumers*

- FTC alleged that **Henry Schein Practice Solutions**, a designer of patient-management systems for dentists, deceptively claimed that its product featured encryption when it actually protected data with a methodology so rudimentary that one vendor agreed to rebrand it as "data camouflage" rather than encryption.[41] The Commission noted that dentists' false confidence in the software's encryption methods may have prevented them from "tak[ing] other reasonable and commercially available steps to protect patients' sensitive personal information."[42]

- In ***ValueClick***, the company stored sensitive information "using only an insecure form of alphabetic substitution that is not consistent with, and less protective than, industry-standard encryption."[43] Because the company had described its products as featuring encryption, FTC found ValueClick's use of non-standard encryption to be a deceptive or misleading practice.

- Similarly, FTC has charged individuals and companies—such as **Sandra Rennert** and **30 Minute Mortgage**—which publicly claim to utilize encryption methods, such as Hypertext Transfer Protocol Secure (HTTPS) or Secure Sockets Layer (SSL), to protect consumer information but do not employ such methods.[44]

---

[40]*See* Complaint at 4 (¶ 8), *In re TRENDNet, Inc.*, No. C-4426 (FTC Jan. 16, 2014) (finding that storing user credentials in clear text on mobile devices and transmitting that information unencrypted violated the company's representations that it adequately protected users' privacy and constituted an unfair trade practice).

[41]*See* Vulnerability Note VU#900031, *Vulnerability Notes Database*, Software Engineering Institute (June 11, 2013), https://www.kb.cert.org/vuls/id/900031.

[42]Complaint at 3 (¶ 10-14), *In re Henry Schein Practice Solutions*, No. C-4575 (FTC May 20, 2016).

[43]Complaint at 13 (¶ 48), *United States v. ValueClick, Inc.*, No. CV08-1711 (C.D. Cal. Mar. 17, 2008).

[44]*FTC v. Rennert*, CV-S-00-0861-JBR (D. Nev. 2000); *FTC v. 30 Minute Mortgage, Inc*., No. 03-60021-CIV (S.D. Fla. Nov. 26, 2003).

- In ***Myspace***, FTC cited the social networking site with sharing information that allowed third-party advertisers to determine a user's full name and other personal information, which it could combine with its tracking cookie and the history of websites that user had visited. This, FTC found, was in direct contradiction to the company's notice to consumers that Myspace would not share personal information with third parties unless the user had expressly permitted Myspace to do so.[45]

2. *Encrypt Sensitive Data When Collected, Transmitted, and Stored Using Industry-Standard Encryption*

- In ***Superior Mortgage***, the company used adequate encryption to secure data submitted through its website, but failed to secure that data as it traveled between the company's various offices. Specifically, the server "was operated by a service provider outside of respondent's computer network," and the information, once collected from the consumer, "was decrypted and emailed to respondent's headquarters and branch offices in clear, readable text."[46]

- In three separate cases (***HTC America***, ***Credit Karma***, and ***Fandango***), FTC pursued § 5 complaints by citing mobile application developers' decisions to turn off the SSL certificate validation feature despite the fact that the iOS and Android guidelines for developers ... explicitly warn[ed] against" doing so.[47]

E. Standard 5: Implement Procedures to Identify and Address Vulnerabilities

Companies cannot claim a lack of awareness about threats to their networks or applications to avoid an enforcement action. FTC has consistently held that companies have an obligation to take basic efforts to understand and protect against the vulnerabilities to

[45] *In re Myspace LLC*, No. C-4369 (FTC Aug. 30, 2012).

[46] Complaint at 3-4 (¶ 13), *In re Superior Mortgage Corp.*, No. C-4153 (FTC Dec. 14, 2005).

[47] FTC, *Start with Security, A Guide for Business: Lessons Learned from FTC Cases* (2015); *In re HTC America Inc.*, No. C-4406 (FTC June 25, 2013); *In re Credit Karma, Inc.*, No. C-4480 (FTC Aug. 13, 2014); Complaint at 4 (¶ 21), *In re Fandango, LLC*, No. C-4481 (FTC Aug. 13, 2014) (noting that the company "could have prevented [the vulnerability] and ensured the secure transmission of consumers' sensitive personal information ... at virtually no cost by simply implementing the default SSL certificate validation settings").

their networks. As an initial matter, FTC has made clear that companies should monitor network traffic and access to databases with sensitive information in order to detect and address weaknesses, employ measures to receive security vulnerability reports, and train employees who handle sensitive data.

1. *Monitor and Control Connections from the Network to the Internet*

- In ***Dave & Buster's***, FTC charged that the company's failure to "employ[] an intrusion detection system and monitor[] system logs" contributed to the exfiltration of 130,000 payment cards from the system after a hacker connected to respondent's networks numerous times without authorization and installed unauthorized software.[48]

- In multiple cases (***LabMD***, ***Franklin's Budget Car Sales***, and ***EPN***), FTC said that monitoring should encompass application activity on employees' workstations to prevent risks such as peer-to-peer software.[49] Such software, which facilitates the sharing of various types of files among users on the internet, has played a significant role in at least three FTC investigations. Specifically, in *LabMD*, the company's billing department manager inadvertently shared approximately 9,300 consumers' names, dates of birth, social security numbers, and healthcare information on the internet. "File integrity monitoring or a more complete walk-around inspection could have detected the [peer-to-peer sharing] program," the Commission found, "but these safeguards were not in place."[50]

2. *Implement Processes to Receive Security Vulnerability Reports*

- In ***HTC America***, FTC noted that the company "failed to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public." Indeed, information developed by security researchers could have helped

[48]Complaint at 2 (¶ 8), *In re Dave & Buster's Inc.*, No. C-4291 (FTC May 20, 2010).

[49]*In re LabMD, Inc.*, No. 9357 (FTC July 28, 2016); *see* Complaint at 3 (¶¶ 9-11), *Franklin's Budget Car Sales, Inc.*, No. C-4371 (FTC Oct. 3, 2012); Complaint at 2 (¶¶ 6-7), *In re EPN, Inc.*, No. C-4370 (FTC Oct. 3, 2012).

[50]*In re LabMD, Inc.*, No. 9357 (FTC July 28, 2016) (slip op. at 13-14).

the programmers avoid the numerous vulnerabilities catalogued in the complaint.[51]

- FTC's enforcement action against **Fandango** focused on the company's failure to establish "a clearly publicized and effective channel for receiving security vulnerability reports." The complaint recounts that a security researcher had emailed the company's customer-service address to warn it that its iOS application did not validate SSL certificates, exposing users to a so-called "man-in-the-middle" attack. Because the email contained the word "password," the customer-service system erroneously categorized the email as a password change request, replied with a message informing the researcher how to reset his password, and marked the inquiry resolved.[52]

3. *Train Employees Handling Sensitive Information on Security Principles*

- The failure to train software developers was at the forefront in ***TRENDNet***. There, FTC attributed the configuration failures that resulted in the inadvertent exposure of users' camera feeds in part to the company's failure to "implement reasonable guidance or training for any employees responsible for testing, designing, and reviewing the security of its IP cameras and related software."[53]

- A broader failure to train employees handling sensitive information has featured in a number of other cases. In ***PLS Financial Services***, FTC charged the company with neglecting to (1) instruct employees to dispose of documents in a manner that prevented reading or reconstructing sensitive information; (2) ensure that employees assigned to collect or transport such information were sufficiently qualified and trained; and (3) notify employees whether information was sensitive and when they should take additional precautions.[54] In ***Eli Lilly & Co.***, the company settled charges that its failure to train employees on consumer privacy and information security resulted in the disclosure of 669 email addresses belonging to subscribers.[55]

---

[51]Complaint at 2, 6 (¶¶ 7, 18), *In re HTC America Inc*., No. C-4406 (FTC June 25, 2013).

[52]Complaint at 3 (¶ 17), *In re Fandango, LLC*, No. C-4481 (FTC Aug. 13, 2014).

[53]Complaint at 5 (¶ 8), *In re TRENDNet, Inc.*, No. C-4426 (FTC Jan. 16, 2014).

[54]Complaint at 5-6 (¶ 17), *United States v. PLS Financial Servs., Inc.*, No. 1:12-cv-8334 (E.D. Ill. Oct. 26, 2012).

[55]Complaint at 6-7, *In re Eli Lilly & Co.*, No. C-4047 (FTC May 8, 2002).

F. Standard 6: Develop and Test New Products and Services with Privacy and Security in Mind

Products, websites, and applications should be designed in accordance with appropriate security standards, and privacy and security features should be tested to ensure they work as intended and are not subject to well-known vulnerabilities. Multiple cases reveal that FTC is focusing enforcement actions on diverse types of missteps by manufacturers and programmers.

- In ***HTC America***, FTC investigated HTC's sale of Android mobile phones with pre-installed applications that circumvented the operating system's permissions-based security model. As a result of vulnerabilities in those applications, sophisticated hackers could access the microphones, send messages, and install other programs on the target phone without the user's consent. More than 18.3 million HTC devices were affected, and the Commission charged that this amounted to an unfair practice in violation of § 5.[56]

- In ***TRENDNet***, the settings of the company's security cameras allowed all users' live feeds to be publicly accessible, regardless of the user's configuration choices. Hackers exploited the vulnerability, and live feeds from nearly 700 cameras became available online for an extended period. FTC alleged that TRENDNet failed to perform adequate security review and testing by, among other things, "verify[ing] that access to data is restricted consistent with a user's privacy and security settings."[57]

- Configuration errors also led to FTC's investigation of **ASUSTeK**. There, the company's routers shipped with default settings that would allow anyone on the internet, with knowledge of the router's IP address, unauthenticated access to files stored on a USB device attached to the router. If the user elected to limit access rights, the installation software recommended credentials such as a user ID and password of "Family" that were highly vulnerable to compromise.[58]

[56]Complaint at 2, 7 (¶¶ 7, 21), *In re HTC America Inc.*, No. C-4406 (FTC June 25, 2013).

[57]Complaint at 5 (¶¶ 9-10), *In re TRENDNet, Inc.*, No. C-4426 (FTC Jan. 16, 2014).

[58]Complaint at 4 (¶¶ 15-18), *In re ASUSTeK Computer Inc.*, No. C-4587 (FTC July 18, 2016).

1. *Assess and Test for Commonly Known Vulnerabilities*

- In ***Guess?***, developers of a web application failed to test for a commonly known vulnerability known as a structured query language (SQL) injection attack. As a result, hackers gained unauthorized access to databases containing consumers' credit card information. The Commission brought a deceptive-practices complaint, alleging that the company's failure to protect against such "commonly known or reasonably foreseeable attacks" amounted to a violation of § 5. It pointed out that the site fell victim to an SQL injection attack in 2002, while "[s]ecurity experts have been warning the industry about these vulnerabilities since at least 1997" and a fix was available to the public at no cost in 1998.[59] Similar actions were filed against **Guidance Software, Inc.**, **Nation's Title Agency**, and **Petco Animal Supplies, Inc**.[60]

- Similarly, in ***Genica Corp. and Compgeeks.com***, FTC alleged that the respondents failed to adequately assess the vulnerability of their web applications and networks to commonly known or reasonably foreseeable attacks or implement readily available defenses to such attacks. For a period of six months, hackers exploited the companies' websites and exported personal information that was stored on the network in clear text.[61] **Ceridian Corp.** and **Life is good, Inc**. received similar complaints.[62]

- As noted above, in *Fandango*, *HTC America*, and *Credit Karma*, FTC has faulted three companies for disabling an SSL certificate validation feature despite the fact that the iOS and Android guidelines for developers "explicitly warn[ed] against" doing so.[63]

For web applications in particular, FTC has identified several kinds of vulnerabilities that it considers to be commonly known and foreseeable. They include cross-site scripting

---

[59]Complaint at 3-4 (¶¶ 9-11), *In re Guess?, Inc.*, No. C-4091 (FTC July 30, 2003).

[60]*In re Guidance Software, Inc.*, No. C-4187 (FTC Mar. 30, 2007); Complaint at 2, 4 (¶¶ 5-6, 13), *In re Nation's Title Agency*, No. C-4161 (FTC June 19, 2006); Complaint at 3, *In re Petco Animal Supplies, Inc.*, No. C-4133 (FTC Mar. 4, 2005).

[61]*In re Genica Corp. and Compgeeks.com*, No. C-4252 (FTC Mar. 16, 2009).

[62]Complaint at 2 (¶¶ 8-9), *In re Ceridian Corp.*, No. C-4325 (FTC June 8, 2011); Complaint at 2 (¶¶ 8-9), *In re Life is good, Inc.*, No. C-4218 (FTC Apr. 16, 2008).

[63]*See In re HTC America Inc*., No. C-4406 (FTC June 25, 2013); *In re Fandango, LLC*, No. C-4481 (FTC Aug. 13, 2014); *In re Credit Karma, Inc.*, No. C-4480 (FTC Aug. 13, 2014).

(*RockYou*), cross-site request forgery, buffer overflow, and multiple password disclosure (*ASUSTeK*), and broken account and session management vulnerabilities (***MTS***).[64]

G. Standard 7: Require Service Providers to Implement Appropriate Security Measures

Companies that make network access or sensitive data available to third parties are responsible for ensuring that the third party has adequate controls in place before providing sensitive data. A number of recent FTC investigations illustrate this point:

- FTC focused an enforcement action against **Upromise** based on a toolbar extension disseminated on its website. The toolbar, which was developed by a service provider, collected "extensive information about consumers' online activities and transmit[ed] it to the service provider for analysis." The toolbar inadvertently collected account numbers and passwords as well, and transmitted them to Upromise in unencrypted text. FTC faulted Upromise for failing to "ensure that its service provider employed reasonable and appropriate measures to protect consumer information and to implement the information collection program in a manner consistent with the respondent's privacy and security policies."[65]

- Similarly, **GMR Transcription** failed to require and verify that its contractor safely transmitted and stored audio files and transcriptions of treatment notes. The contractor in question used File Transfer Protocol for these purposes, and anyone with internet access had unauthenticated access; the files were even indexed by a major search engine. FTC concluded that GMR Transcription's failure to "require [the service provider] by contract to adopt and implement appropriate security measures," and failure to "take adequate measures to monitor and assess whether [the provider] employed measures to appropriately protect personal information under the circumstances," amounted to an unfair trade practice.[66]

---

[64] *See* Complaint at 6 (¶ 16), *United States v. RockYou, Inc.*, No. 12-CV-1487 (N.D. Cal. Mar. 28, 2012) (cross site scripting); Complaint at 2-3 (¶¶ 9 -11), *In re ASUSTeK Computer Inc.*, No. C-4587 (FTC July 18, 2016) (cross-site request forgery, buffer overflow, and multiple password disclosure); Complaint at 3 (¶ 9), *In re MTS, Inc.*, No. C-4110 (FTC May 28, 2004) (broken account and session management vulnerabilities).

[65] Complaint at 2-3, 5 (¶¶ 5, 8-10, 14), *In re Upromise, Inc.,* No. C-4351 (FTC Mar. 27, 2012).

[66] Complaint at 4-5 (¶¶ 11, 21), *GMR Transcription Servs. Inc.*, No. C-4482 (FTC Aug. 14, 2014).

H. Standard 8: Properly Secure Documents, Media, and Devices

In addition to the security of electronic data, a number of FTC enforcement actions stress that the physical security of sensitive information must be protected.

1. *Properly Destroy Documents When No Longer Required*

- **Rite Aid**, for example, was the target of an FTC investigation because it did not "implement policies and procedures to dispose securely of [personal] information, including, but not limited to, policies and procedures to render the information unreadable in the course of disposal." As a result, personal records were discarded in dumpsters and FTC charged Rite Aid with an unfair trade practice.[67] **American United Mortgage Co.** and **CVS Caremark Corp.** were charged with similar unfair practices.[68]

2. *Securely Store Sensitive Records and Other Printed Information*

- In ***Navone***, a business owner was charged in his personal capacity for storing 40 boxes of information derived from credit reports in his garage and later improperly disposing of the information. FTC alleged that he neither informed service providers of the sensitive nature of the records nor ensured their secure storage or disposal.[69]

3. *Securely Store Sensitive Information During Transport*

- In ***Cbr Systems***, backup tapes, a laptop, and a USB drive were stolen from an employee's car as the employee transported those items between Cbr facilities. The devices were unencrypted, and they contained a wide variety of personal information on Cbr's clients as well as network credentials. FTC brought a deception case against the company for, among other things, "transporting portable media containing personal information in a manner that made the media vulnerable to theft or other misappropriation" and failure to ensure the back-up data was encrypted.[70]

---

[67]Complaint at 2-3 (¶¶ 7-8), *In re Rite Aid Corp.*, No. C-4308 (FTC Nov. 12, 2010).

[68]*United States v. American United Mortgage Co*., No. 07-cv-7064 (N.D. Ill. Dec. 17, 2007) (company left loan documents with personal information in an unsecured dumpster); Complaint at 2-3 (¶¶ 7-8), *In re CVS Caremark Corp.*, No. 4259 (FTC June 18, 2009) (improper disposal of pharmacy records).

[69]*FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 30, 2009).

[70]Complaint at 2-3 (¶¶ 9, 12), *In re Cbr Systems, Inc.*, No. C-4400 (FTC Apr. 29, 2013).

CONCLUSION

To minimize the risk of being the subject of an FTC data-security enforcement action, companies should remain cognizant of past enforcement actions and related best practices, and practice security-by-design. As FTC highlighted in its recent guidance, factoring security into decision-making in every facet of a business will reduce the likelihood of an incident that could result in an FTC enforcement action or a costly data breach.[71] The security-by-design approach requires consideration of data security at every stage of doing business. This includes, among other steps, determining what information to collect from consumers; how information should be collected, stored, and transmitted; and who within the company will be allowed to access that information. Companies should also consider data security when establishing their networks and web applications, developing new products, and engaging with service providers. The lapses in data security described in the FTC enforcement actions above—and the eight standards derived therefrom—serve as a helpful roadmap for companies to evaluate and improve their data-security practices.

[71] FTC, *Start with Security, A Guide for Business: Lessons Learned from FTC Cases* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.