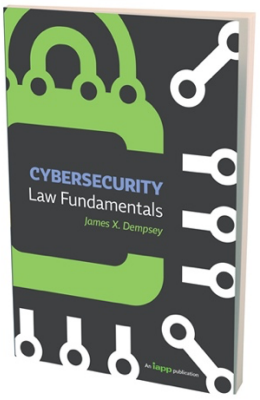
Federal Cybersecurity Enforcement – The Federal Trade Commission

Chapter 10 from *Cybersecurity Law Fundamentals* (2021)

By James X. Dempsey

The Federal Trade Commission is the nation's de facto cybersecurity regulator. Using its authority under Section 5 of the Federal Trade Commission Act, it has built a "common law" of cybersecurity, case-by-case, through enforcement actions alleging that the failure to apply reasonable security practices to protect personal information is an unfair or deceptive trade practice. The evolution of the FTC's authority and the implications of the long lists of security failings it has alleged in its complaints and the long lists of security measures it has detailed in its settlement orders are described in Chapter 10 of *Cybersecurity Law Fundamentals*, reprinted below. But first, here are updates from CybersecurityLawFundamentals.com:



10.1 Overview - The Origins and Evolution of FTC Cybersecurity Enforcement

On January 4, 2022, the FTC issued a blog post warning companies to remediate the Log4j security vulnerability, which was ubiquitous at the time: "It is critical that companies and their vendors relying on Log4j act now, in order to reduce the likelihood of harm to consumers, and to avoid FTC legal action." The warning was significant in itself, in that I do not recall the FTC making such an express statement on a specific security measure—almost a directive—outside of its press releases and compilations drawing lessons from enforcement actions. Moreover, the post included a quite definitive statement of the FTC's view that there is a general duty to mitigate vulnerabilities: "The duty to take reasonable steps to mitigate known software vulnerabilities implicates laws including, among others, the Federal Trade Commission Act and the Gramm Leach Bliley Act." I'm not sure the FTC had ever used the word "duty" in this way. ("Duty" is also an important concept under negligence law. The FTC's authority under Section 5 of the FTC Act shares some similarities with the cost-utility analysis at the core of negligence law.) The blog went on to say: "The FTC intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future." Note as well the re-emergence of the word "reasonable."

10.4.5 Fines and Penalties

In response to *AMG Capital Management*, the FTC has invoked a unique process under the FTC Act to partially restore its ability to impose monetary penalties. Under Section 5(m)(1)(B) of the Act, 5 U.S.C. 45(m)(1)(B), the FTC may notify companies that certain acts or practices have been found in administrative decisions, other than consent orders, to be deceptive or unfair. Companies that receive such a "Notice of Penalty Offenses" then have "actual knowledge" that those practices violate the law. If a company engages in that conduct in the future, even though it was not a party to the initial proceeding that declared the practice illegal, Section 5(m)(1)(B) allows the FTC to sue the company, seeking civil penalties. In October 2021, the FTC began sending large numbers of such notices, starting with for-profit educational institutions listing deceptive employment and earnings claims and then warning an array of

large companies, top advertisers, leading retailers, top consumer product companies, and major advertising agencies about the use of endorsements. As of early December 2021, the FTC had not used the same tactic with regards to cybersecurity, and it is not clear whether it can do so, because almost all FTC cybersecurity enforcement actions have resulted in a consent order, for which the Section 5(m)(1)(B) is not available, but the issue merits monitoring.

10.4.7 GLBA Safeguards: The Next Generation

In October 2021, the FTC adopted the amendments to the GLBA Safeguards Rule described in the book. The new rule is considerably more detailed in terms of the elements required in an information security plan. See revisions to Chapter 9.2.10.1.

10.4.10 FTC Rulemaking

Under Section 18 of the Federal Trade Commission Act, 15 U.S.C. § 57a, the Commission may prescribe--

> (A) interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices in or affecting commerce (within the meaning of section 45(a)(1) of this title), and
>
> (B) rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce (within the meaning of section 45(a)(1) of this title) … .

This language and specific procedures that go beyond the Administrative Procedure Act were added to the FTC Act by the Magnuson-Moss Warranty-Federal Trade Commission Improvement Act of 1975. The statute's unique rulemaking procedures are referred to as "Mag-Moss."

For decades, Mag-Moss procedures had been presumed to be so cumbersome as to be impossible to use. However, in 2020, Commissioner Rebecca Kelly Slaughter began arguing that the real impediments to effective rulemaking came not from the statute but from self-imposed requirements. She argued: "With revised Rules of Practice, the Commission would be well positioned to initiate Mag-Moss rule-makings designed to curb problematic data abuses." In July 1, 2021, under its new chair, Lina Khan, the FTC voted, 3-2, to streamline its Mag-Moss rulemaking procedures, essentially adopting Commissioner Slaughter's concept. Meanwhile, in June 2021, Commissioner Wilson, a Republican traditionally opposed to rulemaking for privacy, stated that, "… in the absence of Congressional action, I have reluctantly come to consider whether we [the FTC] should begin a privacy rulemaking proceeding." And in Executive Order 14036, *Promoting Competition in the American Economy*, President Biden "encouraged" the FTC chair, "in the Chair's discretion," to exercise the FTC's "statutory rulemaking authority, as appropriate and consistent with applicable law," to establish rules on "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."

All of this started to come together in late 2021 when the FTC informed the Office of Management and Budget that it was "considering initiating a rulemaking under section 18 of the FTC Act to curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination." The Commission indicated that it was aiming to issue an Advanced Notice of Proposed Rulemaking in February 2022.

Last updated: January 21, 2022

CHAPTER 10

Regulatory Enforcement—The Federal Trade Commission

Practice Tips

- The FTC is the nation's de facto cybersecurity regulator with respect to the protection of personal information.
- The commission has claimed this role for itself based on both the unfair and deception prongs of its authority under Section 5 of the FTC Act. Promising consumers security and failing to deliver is deception, and in the commission's view it is unfair to collect personal information and fail to protect it with reasonable safeguards.
- A breach is not per se a violation of Section 5; instead, it gives the FTC an opening to examine all aspects of an entity's handling of data.
- The FTC's authority to regulate cybersecurity under an unfairness theory is actually not that clear, but it has survived both major challenges it has faced, in the *Wyndham* and *LabMD* cases.
- The *LabMD* case led to a major change in the FTC's cybersecurity orders and settlements, with the commission imposing much more detailed and technologically specific requirements on respondents.
- The FTC has defined cybersecurity obligations not by regulation, but rather through case-by-case enforcement actions.

- The allegations in the FTC's enforcement complaints can be read as a catalogue of what is unfair, and the security measures imposed in its settlements and orders can be read as a list of what measures are needed to provide "reasonable cybersecurity," but the commission seems to take a totality of the circumstances approach, under which what is reasonable security in any context will depend on a cost-benefit analysis unique to that entity.
- The Supreme Court decided in *AMG Capital Management, LLC v. FTC* that the commission cannot demand monetary relief such as restitution in its court cases.
- The FTC has proposed major revisions to its Safeguards Rule under the GLBA.

10.1 Overview—The Origins and Evolution of FTC Cybersecurity Enforcement

In June 2001, an employee at the pharmaceutical company Eli Lilly made a careless mistake. Eli Lilly, the maker of Prozac, offered a service whereby users of its drugs could sign up for an email alert notifying them that it was time to refill their prescriptions. Only 669 people had signed up for the service. Maybe for that reason Eli Lilly decided to discontinue the program. An employee was told to send an email to program subscribers advising them that the service was being discontinued. In creating the email, the employee did not realize that he was including the addresses of all 669 customers in the "to" line. On June 27, 2001, when that employee hit "send" on that email to 669 customers, he helped set in motion, like the proverbial butterfly beating its wings, a chain of events that has resulted in the FTC becoming the nation's de facto cybersecurity regulator.

Sixteen years later, in September 2017, Equifax disclosed that it had suffered a data breach. The attackers stole, by Equifax's own count, 147 million names and birthdates, 145.5 million Social Security numbers, 99 million physical addresses, 20.3 million telephone numbers, 17.6 million

email addresses, and 209,000 payment card numbers and expiration dates, among other things.

While the Equifax breach affected more than 200,000 times more people than the Eli Lilly data spill, and although Equifax was just the latest in a long string of high-profile breaches, the FTC had no more statutory authority over cybersecurity in 2017 than it had in 2002 when it responded to the Eli Lilly incident with its first cybersecurity enforcement action. But the FTC's *use* of that authority has expanded remarkably, after weathering judicial challenges.

The FTC's cybersecurity framework for Eli Lilly, Equifax, and most of the economy is based on a clause in Section 5 of the FTC Act, "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful," adopted in 1938. This authority has been implemented by the FTC through case-by-case investigations that have resulted, almost always, in agreed settlements. From 2002 through about 2016, the requirements imposed on companies by the commission—whether acting under its unfair and deceptive authority or under the specific authority granted it for the financial services sector and children—were remarkably simple and consistent over time, consisting of general mandates to companies to adopt "reasonable" safeguards, without a lot of detail.

In 2018, the U.S. Court of Appeals for the Eleventh Circuit cast considerable doubt on the FTC's approach. The FTC had brought a Section 5 administrative enforcement action against a company called LabMD. Unlike almost every other target of FTC enforcement (the other notable exception being Wyndham Hotels), LabMD fought the FTC every step of the way, ultimately appealing the commission's final order to the Eleventh Circuit. In June 2018, the Eleventh Circuit declared the commission's order unenforceable and vacated it. *LabMD, Inc. v. FTC*, 894 F.3d 1221 (11th Cir. 2018). The court's opinion delighted defense counsel, but at the end of the day, the ruling was fairly narrow: The court accepted as a premise that the FTC's unfairness authority encompassed the failure to provide cybersecurity, and it did not question the FTC's conclusion that the exposure of personal information was itself sufficient harm for the commission to act. Instead, it held that the FTC's order was invalid because it was not specific enough.

When the Eleventh Circuit opinion was handed down, in June 2018, the commission was in transition. A new chair nominated by President

Trump had just been confirmed in April 2018. The commission received its full complement of commissioners in September 2018. It was uncertain how the Republican-controlled commission would view its cybersecurity authority.

In June 2019, we received an answer when the commission announced a settlement with Lightyear Dealer Technologies. In response to *LabMD*, and probably also in response to growing concerns about cybersecurity, the commission was going to be more specific in its cybersecurity orders—much more specific. While keeping the framework it had imposed on Eli Lilly and all subsequent respondents, it would delete the word "reasonable" from its remedies and add additional detail in terms of specific security technologies and practices that had to be adopted.

In the Lightyear case, these included requiring encryption of certain information, vulnerability testing of its network once every four months, and the adoption of data access controls for all databases storing personal information, including by, at a minimum: (1) restricting inbound connections to approved IP addresses; (2) requiring authentication to access them; and (3) limiting employee access to what is needed to perform that employee's job function.

The Lightyear settlement was followed a month later by settlement of the massive Equifax breach, with even more detailed remedial measures, nearly two dozen in total, including patch management procedures requiring confirmation that patches were actually completed, the use of secure development practices for applications developed in-house, and adoption of a process for receiving and addressing vulnerability reports from third parties.

Lightyear and Equifax both settled with the FTC, meaning there was no court review of the FTC's new approach. Whether the commission's more detailed orders would satisfy the concerns articulated by the Eleventh Circuit in *LabMD* must await a future respondent willing to fight all the way.[1] For now, the Lightyear and Equifax settlements provide the template for how the FTC's views its cybersecurity jurisdiction and what it views as necessary in order to avoid being found to engage in

1 The lawyers who represented both Wyndham and LabMD are ready. See Doug Meal, Michelle Visser and David Cohen, *FTC Exceeded Its Authority In Zoom Cybersecurity Settlement*, Law360 (Nov. 17, 2020); Doug Meal, Michelle Visser, David Cohen and Joseph Santiesteban, *FTC Data Security Consent Orders Are New But Not Improved*, Law360 (March 23, 2020).

unfair practices for failing to adequately protect collected information about individuals.

Where the FTC has had express authority over cybersecurity, specifically with regard to financial institutions under the GLBA, its approach so far has followed the same trajectory as its enforcement actions, from general process-oriented standards to more specific requirements. The initial GLBA rule, issued in 2002, focused on process-oriented requirements very similar to those imposed on Eli Lilly. Fast forward to 2019: While the FTC was negotiating its settlements with Lightyear and Equifax, it was drafting revisions to its Safeguards Rule for financial services companies under the GLBA. The proposed rule was published in March 2019. The proposed revisions, discussed near the end of this chapter, would include specific requirements, similar to those in the Lightyear and Equifax settlements.

The path that the FTC started down in 2002 with Eli Lilly has been followed by other regulatory agencies: The FCC, SEC, and the Consumer Financial Protection Bureau all have invoked general statutory language to claim cybersecurity enforcement powers. (The FCC did have Section 222 of the Communications Act, which does mention protecting the confidentiality of customer data.) The results have been very limited in the case of the CFPB and quite limited in the case of the FCC but more robust in the case of the SEC. See Chapter 11. This process of regulatory activism has taken place in the context of congressional inaction and a private litigation system, with its preference for settlements, that is not effective in generating systemic change or even in producing judicial rulings of precedential value.

Since the evolution of the FTC's approach helps explain the current situation, it is worth going back to the beginning.

10.2 Section 5 of the FTC Act

Section 5 of the FTC Act declares that "unfair or deceptive acts or practices in or affecting commerce" are unlawful. 15 U.S.C. § 45(a).

In 1994, Congress adopted Subsection (n) of Section 5, cabining the FTC's unfairness authority:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an

> act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

"[T]he relevant inquiry here is a cost-benefit analysis." *FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 236, 255 (3d Cir. 2015). The language leaves substantial room for action against conduct that causes or is likely to cause substantial injury to consumers, but it leaves unanswered the question of what is "injury."

As for its deception authority, the commission in 1983 adopted a policy statement[2] stating that it would consider a representation, omission, or practice to be deceptive if it is likely to mislead consumers, considered from the perspective of a reasonable consumer, and material, that is, likely to affect consumers' choice or conduct regarding a product or service.

The commission has two ways to bring an enforcement action: Under Section 5(b), it can file an administrative complaint and, after a hearing, issue a cease and desist order. Alternatively, under Section 13(b) of the FTC Act, it can bring a complaint in District Court seeking injunctive relief against an entity that "is violating, or is about to violate, any provision of law enforced" by the commission. It has used both approaches in cybersecurity cases.[3]

Since 2002, the FTC has invoked Section 5 to bring more than 60 data security enforcement actions. Initially, the FTC used the deception prong of its Section 5 authority to address cybersecurity, bringing enforcement

2 FTC, *Policy Statement on Deception* (Oct. 14, 1983) https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf, *archived at* https://perma.cc/C2MH-5UDC.

3 For the FTC's own summary of its authorities and procedures, see *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority* https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (Oct. 2019), *archived at* https://perma.cc/C6XK-C7JR.

actions against companies that had stated, in their privacy policies or other statements to consumers, that they protected consumers' data. Later, the FTC began relying also on unfairness, in effect taking the position that it is an unfair trade practice to collect personal information and not protect it with reasonable security measures.

10.3 The Evolution of the FTC's Cybersecurity Strategy—GLBA Safeguards Rule

The FTC's strategy in applying Section 5 to cybersecurity did not grow out of the Eli Lilly case in isolation. Nor was it dictated solely by the FTC's lack of rulemaking authority over cybersecurity. To the contrary, there was a tight connection between the FTC's Section 5 proceedings and its rulemaking for the financial services sector under the GLBA.

Under GLBA, the financial regulators, including the FTC, were specifically directed by Congress to "establish appropriate standards … relating to administrative, technical, and physical safeguards—(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." Despite the scope of that mandate, the agencies adopted relatively short and simple rules focused on the *process* of information security rather than on technological substance.[4]

The "financial institutions" subject to the FTC's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under Section 505 of the GLBA, 15 U.S.C. § 6805. More specifically, those entities include but are not limited to mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account

4 The FTC issued an Advanced Notice of Proposed Rulemaking under GLBA in September 2000. It issued a proposed rule in August 2001, and in May 2002 it promulgated the final Safeguards Rule, to take effect in 2003. *Standards for Safeguarding Customer Information; Final Rule—16 CFR Part 314 (May 23, 2002)* https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf, *archived at* https://perma.cc/EBG4-TNGV.

servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the SEC, and entities acting as finders. 16 C.F.R. § 313.1(b).

The Safeguards Rule adopted by the FTC in 2002 under GLBA requires financial institutions to:

> develop, implement and maintain a comprehensive written information security plan that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. 16 C.F.R. § 314.3(a).

The FTC rule goes on to say, in 16 C.F.R. § 314.4, that, in order to develop, implement and maintain such a plan, entities shall:

- Designate an employee or employees to coordinate the program.
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.
- Assess the sufficiency of any safeguards in place to control these risks.
- At a minimum, such a risk assessment shall consider risks in:
    - Employee training and management.
    - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal.
    - Detecting, preventing and responding to attacks, intrusions, or failures.
- Design and implement information safeguards to control the risks identified.
- Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, system and procedures.

- Oversee service providers by:
    - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards.
    - Requiring service providers by contract to implement and maintain such safeguards.
- Evaluate and adjust the program in light of the results of the required testing and monitoring or any other material changes.[5]

Note the lack of technological details: a regulated entity must assess its risks, but the rule doesn't suggest in any detail what those risks might be, and it must adopt safeguards commensurate with those risks, but there is no requirement to use any specific security technology or practice (other than to regularly test or otherwise monitor the effectiveness of key controls, system and procedures).

In March 2019, the FTC announced that it was seeking comment on proposed amendments to the GLBA Safeguards Rule, but more on that in Chapter 10.4.7 below.[6]

5 Guidelines adopted jointly by the other regulators included the additional element of requiring financial institutions to consult with their Boards of Directors at key stages of the process of developing and implementing their information security program. See Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; and Office of Thrift Supervision, Treasury, *Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness*, 66 Fed. Reg. 8616-8641 (Feb. 1, 2001) https://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010117/attachment.pdf, *archived at* https://perma.cc/2CQ5-5QNA.

6 The Notice of Proposed Rulemaking was officially published in the Federal Register on April 4, 2019. FTC, *Standards for Safeguarding Customer Information—Notice of Proposed Rulemaking,* 84 Fed. Reg. 13158 (Apr. 4, 2019) https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information*, archived at* https://perma.cc/ZU3C-82PK.

10.4 From *Eli Lily* to *Equifax*: Case-by-Case Enforcement Under Section 5

While the FTC was drafting its first GLBA Safeguards Rule, it was also plotting its enforcement strategy for entities *not* covered by specific statute. To address the rest of the economy, it turned to the only statute it had, Section 5 of the FTC Act: "… unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a).

10.4.1 Cybersecurity Deception

10.4.1.1 Affirmative Misrepresentation

The FTC's first cybersecurity case was Eli Lilly.[7] In its complaint, the FTC quoted promises the company had made on its website to "respect the privacy of visitors," "maintain our guests' privacy," and " protect the confidentiality" of consumer information. The specific failings alleged by the FTC complaint mainly related to the circumstances of the sending of that one mistaken email: "For example, respondent failed to provide appropriate training for its employees regarding consumer privacy and information security; failed to provide appropriate oversight and assistance for the employee who sent out the email, who had no prior experience in creating, testing, or implementing the computer program used; and failed to implement appropriate checks and controls on the process, such as reviewing the computer program with experienced

7 There was one case from 2000 that almost qualified as the first FTC data security case. In *FTC v. Sandra L. Rennert*, filed in the federal district court in Nevada, the FTC alleged that defendants, who sold Viagra and other drugs online, had represented to consumers, expressly or by implication, that the information customers provided to their Web sites was encrypted and that defendants used an SSL secure connection when transmitting this information over the Internet. The FTC alleged that, in fact, the information customers provided to defendants' Web sites was not encrypted and defendants did not use an SSL secure connection when transmitting this information over the Internet. However, when the FTC settled the case, the security issues were not addressed. The case suggests, however, that the FTC was seeking security enforcement cases as early as 2000. *FTC v. Sandra L. Rennert,* Complaint for Permanent Injunction and Other Equitable Relief (D. Nev.) https://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm, *archived at* https://perma.cc/M523-Z8W9. See also FTC, *Online Pharmacies Settle FTC Charges* (July 12, 2000) https://www.ftc.gov/es/node/64217, *archived at* https://perma.cc/F6YM-SPVR.

personnel and pretesting the program internally before sending out the email."[8]

In Eli Lilly, the FTC had plenty of allegedly deceptive statements to hang its hat on, and it did not separately allege unfairness. However, in its settlement with Eli Lilly, the FTC did not only order the company to not misrepresent in any manner, expressly or by implication, the extent to which it maintains and protects data privacy or confidentiality. The FTC also imposed remedies that closely tracked the safeguards it was, at that precise time, adopting for the financial services entities under its jurisdiction. (The FTC issued its GLBA ANPR in September 2000, its proposed rule in August 2001, and its final rule in May 2002. The Eli Lilly incident occurred in 2001 and the FTC's order was issued in May 2002). After ordering Eli Lilly not to make any further misrepresentations about its security practices, the commission ordered the company to establish and maintain an "information security program" for the protection of consumer information:

> Such program shall consist of:
>
> > A. designating appropriate personnel to coordinate and oversee the program;
> >
> > B. identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information, including any such risks posed by lack of training, and addressing these risks in each relevant area of its operations, whether performed by employees or agents, including: (i) management and training of personnel; (ii) information systems for the processing, storage, transmission, or disposal of personal information; and (iii) prevention and response to attacks, intrusions, unauthorized access, or other information systems failures;
> >
> > C. conducting an annual written review by qualified persons, which shall monitor and document compliance with the program, evaluate the program's effectiveness, and recommend changes to it; and

8 *In the Matter of Eli Lilly and Co.*, Docket No. C-4047, Complaint (May 8, 2002) https://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillycmp.htm*, archived at* https://perma.cc/3MTU-VMJD.

> D. adjusting the program in light of any findings and recommendations resulting from reviews or ongoing monitoring, and in light of any material changes to its operations that affect the program.

The order remains in effect for 20 years.

Several aspects of the FTC's approach in the Eli Lilly cases stand out: First, the FTC did not confine its investigation to identifying what caused the breach. Once data spilled and the FTC got involved, it looked broadly at the company's data security practices. Second, the FTC did not tie the agreed-upon remedies to correcting the flaw that led to the breach. Instead, it ordered the company to improve its cybersecurity practices overall, in ways that went well beyond the failure that caused the leak. Both of these continue to characterize the FTC's approach to cybersecurity today. Finally, the FTC did not order Eli Lilly to take any particular steps to improve its cybersecurity. Instead, the commission imposed a set of procedural obligations, ordering Eli Lilly to identify risks and to address them, in each relevant area, including training. These obligations directly tracked the GLBA Safeguards Rule:

GLBA Safeguards Rule (2002)	Eli Lilly Settlement (2002)
Develop, implement, and maintain comprehensive written information security plan with appropriate administrative, technical, and physical safeguards.	Establish and maintain information security program.
Designate employee(s) to coordinate.	Designate personnel to coordinate.
Identify reasonably foreseeable risks, including risks in employee training, info systems, incident detection, prevention, and response.	Identify reasonably foreseeable risks.
Design safeguards to control risks.	Address risks identified, including training, info systems, incident prevention, and response.
Regularly test or monitor effectiveness.	Conduct annual written review by qualified persons to monitor and document compliance.

Oversee service providers.	"Whether by employees or agents."
Evaluate and adjust.	Evaluate effectiveness and adjust.

One last point: All of the items in the Eli Lilly settlement appear in FTC cybersecurity settlements today. As a result of the *LabMD* case and probably driven as well by the rising tide of cybersecurity concern, the FTC is now adding many much more specific requirements to its settlements and orders, but the Eli Lilly elements are still visible.

The FTC continues to bring pure deception cases involving cybersecurity. Recent examples include its 2020 case against Tapplock, which involved an IoT device, specifically, internet-connected and fingerprint-enabled padlocks ("smart locks");[9] its district court action against Office Depot, which resulted in the company agreeing to pay more than $34 million in refunds;[10] and its 2018 complaint against Uber.[11]

10.4.1.2 Failure to Disclose Vulnerabilities

In cases against Oracle and others, the FTC has taken the position that the failure to disclose can be deceptive. The Oracle case, settled in 2016, involved Oracle's Java computing platform, the consumer version of which had been installed on more than 850 million personal computers.[12] The FTC's case was based on the allegation that Oracle had deceived customers by failing to disclose or disclose adequately that updating Java SE would not delete or replace all older iterations of Java SE on a consumer's computer, and as a result, a consumer's computer could

9 *In the Matter of Tapplock, Inc.*, Complaint and Decision and Order (May 20, 2020) https://www.ftc.gov/enforcement/cases-proceedings/192-3011/tapplock-inc-matter, *archived at* https://perma.cc/55HR-P9BU.

10 The complaint and settlement in *Federal Trade Commission v. Office Depot, Inc.,* are available at https://www.ftc.gov/enforcement/cases-proceedings/172-3023/office-depot-inc, archived at https://perma.cc/5ZSS-4QDP.

11 *In the Matter of Uber Technologies, Inc.,* Complaint (Oct. 26, 2018) https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_complaint.pdf. For all documents in the case, see https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc.

12 Materials in the case are available at https://www.ftc.gov/enforcement/cases-proceedings/132-3115/oracle-corporation-matter, *archived at* https://perma.cc/QL7U-MJAN.

still have iterations of Java SE installed that were vulnerable to security risks. Oracle accepted a settlement that ordered it not to misrepresent the privacy or security on any consumer software, provide clear and conspicuous notice to consumers during the Java SE update process if they have outdated versions of the software on their computer, notify them of the risk of having the older software, and give them the option to uninstall it.

Another failure to disclose case was brought against Lenovo, which the FTC alleged had failed to disclose or disclose adequately that a third-party app Lenovo installed on its computers would act as a man-in-the-middle between consumers and all websites with which they communicated, including sensitive communications with encrypted https:// websites, and would collect and transmit consumer internet-browsing data to the app developer. In addition to prohibiting any misleading representations about its software and requiring affirmative express consent before installing certain software, the order also required Lenovo to implement a comprehensive software security program reasonably designed to (1) address software security risks related to the development and management of new and existing software; and (2) protect the security, confidentiality, and integrity of covered information, with specific elements similar to those in the Eli Lilly order.[13]

10.4.2 Cybersecurity Failures as Unfair

10.4.2.1 Failure to Encrypt and Take Other Affirmative Measures

In Eli Lilly and other early data security cases, the FTC alleged that the respondent was both deceptive and unfair. In 2005, in a proceeding against BJ's Wholesale Club, the FTC brought its first data security case under a pure unfairness theory.[14] BJ's, a retailer, had failed to encrypt

13 *In the Matter of Lenovo (United States) Inc.,* Decision and Order (Jan. 2, 2018) https://www.ftc.gov/system/files/documents/cases/152_3134_c4636_lenovo_united_states_decision_and_order.pdf, *archived at* https://perma.cc/UKY9-8X4S.

14 *In the Matter of BJ's Wholesale Club, Inc.,* Docket No. C-4148, Complaint (Sept.23, 2005) https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf, *archived at* https://perma.cc/J45V-L3AS.

consumer information when it was transmitted over its wireless network or stored on computers in its stores. The FTC also alleged that BJ's:

- Stored the information in files that could be accessed using a commonly known default user ID and password.
- Failed to use readily available security measures to limit access to its computer networks through wireless access points.
- Failed to use measures to detect unauthorized access to its networks.
- Stored data longer than necessary.

Like Eli Lilly, BJ's settled, and the settlement required BJ's to establish and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards with provisions essentially identical to those in Eli Lilly.[15]

Eli Lilly (2002)	BJ's Wholesale (2005)
Establish and maintain info security program.	Establish, implement, and maintain comp. written info security program *reasonably* designed to protect consumer data, with appropriate administrative, technical, and physical safeguards.
Designate personnel to coordinate.	Designate employee(s) to coordinate and be accountable.
Identify reasonably foreseeable risks.	Identify material internal and external risks—training, info systems, and prevention, detection and response.
Address risks identified, including training, info systems, incident prevention and response.	Design and implement *reasonable* safeguards to control risks identified.
	Conduct annual written review by qualified persons to monitor and document compliance.

15 *In the Matter of BJ's Wholesale Club, Inc.,* Docket No. C-4148, Decision and Order (Sept.23, 2005) https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305do0423160.pdf, *archived at* https://perma.cc/86R4-JUK4.

Conduct annual written review by qualified persons to monitor and document compliance.	Obtain assessment from qualified, objective, independent third-party professional every two years.
"Whether by employees or agents."	
Evaluate effectiveness and adjust.	Evaluate and adjust.
Order remains in effect 20 years.	Order remains in effect 20 years.

Note: The settlement does not require BJ's to encrypt customer data, adopt robust passwords, or limit how long it stored data, specific points alleged in the compliant. Note also the settlement included the concept of reasonableness: The comprehensive information security program had to be "reasonably designed" to protect consumer data and had to include "reasonable safeguards" to control the risk identified in a required risk assessment. Reasonableness remained an express element of subsequent FTC orders, through *LabMD*.

10.4.2.2 Failure to Require Cybersecurity of Service Providers

The Eli Lilly settlement included a phrase requiring the company to address cybersecurity risks in each relevant area of its operations, "whether performed by employees or agents." In subsequent cases, the FTC specifically alleged that the failure to oversee the cybersecurity practices of service providers was an unfair act or practice.

One case involved GMR Transcription Services, which transcribed audio recordings for a variety of clients. GMR hired independent service providers to do the work. One of these service providers, Fedtrans, in turn further outsourced the work to individual typists. Fedtrans used an insecure application to store medical audio and transcript files and transmit them to its typists in clear readable text; worse, the application was configured so that the files could be accessed online by anyone without authentication. The FTC complaint alleged that GMR had failed to:

- Require typists to adopt and implement security measures, such as installing antivirus applications, or confirm that they had done so.

- Adequately verify that the service provider, Fedtrans, implemented reasonable and appropriate security measures to protect personal information in audio and transcript files on Fedtrans' network and computers used by Fedtrans' typists.

Specifically, GMR had failed to require Fedtrans by contract to adopt and implement appropriate security measures to protect personal information, such as by requiring that files be securely stored and securely transmitted to typists (e.g., through encryption) and authenticating typists (e.g., through unique user credentials) before granting them access to such files, and take adequate measures to monitor and assess whether Fedtrans employed measures to appropriately protect personal information.

The settlement, in addition to containing the basic elements of the Eli Lilly framework, also included a provision similar to the one in the GLBA Safeguards Rule:

> the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondents, and requiring service providers by contract to implement and maintain appropriate safeguards[16]

Note: The practice mandated in the GMR proceeding—that any entity that uses a third party to process data on its behalf must exercise due diligence control over the security practices of that service provider—is now widely required. In addition to being in the GLBA Safeguards Rule, it is reflected in the audit priorities of the SEC's Office of Compliance Inspections and Examinations, in the reliability standards approved by the Federal Energy Regulatory Commission, and in various state laws, among other frameworks.

16 Other cases where the FTC alleged that companies failed reasonably to oversee the security practices of their service providers include *In the Matter of BLU Products*, FTC No. 1723025, Complaint (April 30, 2018), https://www.ftc.gov/enforcement/cases-proceedings/172-3025/blu-products-samuel-ohev-zion-matter; *In the Matter of Lenovo, Inc.,* FTC No. 1523134 (Sept. 13, 2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3134/lenovo-inc, *archived at* https://perma.cc/JGW4-N2GR; and *In the Matter of Upromise, Inc.,* FTC No. 1023116 (April 3, 2012), https://www.ftc.gov/enforcement/cases-proceedings/102-3116/upromise-inc, *archived at* https://perma.cc/7FZD-CARU.

It is now generally established practice that an entity seeking to outsource any data-processing function requires the third-party vendor to complete a questionnaire on its cybersecurity practices, and many service contracts contain a clause addressing the cybersecurity obligations of the service provider. Service providers often respond with a "SOC report."[17]

10.4.2.3 Failure to Require Cybersecurity of End Users of Consumer Data

In 2011, the FTC obtained settlements with several companies, sometimes referred to as resellers, that bought credit reports from consumer reporting agencies and resold them to mortgage brokers and others to use in determining consumers' eligibility for credit.[18] The FTC alleged that the resellers were "financial institutions" as that term is defined by Section 509(3)(A) of the GLBA, 15 U.S.C. § 6809 (3)(A), and therefore subject to the requirements of the GLBA Safeguards Rule, so the commission alleged violations of both the FTC Act and GLBA, as well as the Fair Credit Reporting Act.

The resellers had not been breached, and the FTC made no allegation about the security of the resellers' computer networks. Rather, the FTC alleged, it was the clients of the resellers who had poor security practices, which hackers exploited to access more than 1,800 credit reports via those clients' computer networks. The complaints alleged that the resellers failed to provide "reasonable and appropriate security for consumers' personal information," by failing to:

- Assess the risk of allowing end users with unverified or inadequate security to access consumer reports.
- Evaluate the security of end user's computer networks.
- Require end users to implement appropriate information security measures.

17 See KPMG, *Effectively using SOC 1, SOC 2, and SOC 3 reports for increased assurance over outsourced operations* (2012) https://info.kpmg.us/content/dam/advisory/en/pdfs/risk-assurance/effictively-using-soc.pdf, *archived at* https://perma.cc/4VBK-QUC5.

18 FTC, *Credit Report Resellers Settle FTC Charges; Security Failures Allowed Hackers to Access Consumers' Personal Information* (Feb. 3, 2011) https://www.ftc.gov/news-events/press-releases/2011/02/credit-report-resellers-settle-ftc-charges-security-failures, *archived at* https://perma.cc/M6F8-VZP2.

- Train end user clients.
- Monitor access by end users, including by monitoring to detect anomalies.
- Correct existing vulnerabilities or threats in light of known risks.

The FTC also alleged that the resellers allowed clients without basic security measures in place, such as firewalls and updated antivirus software, to have access to the consumer reports.[19]

Again, the settlement order included all of the elements in *Eli Lilly* but also required the resellers to address the security practices of their customers, the end users of the data:

> IT IS ORDERED that respondent shall … establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers, including the security, confidentiality, and integrity of personal information accessible to end users.

10.4.2.4 Failure to Provide Adequate Security in Software or Devices

The FTC has obtained settlements against companies that did not themselves collect consumer information but instead produced software or devices that put data at risk.

For example, in January 2016, the FTC reached a settlement agreement with Henry Schein Practice Solutions, a company that make office management software for dental practices.[20] The FTC alleged that the company had misrepresented that its software encrypted patient data.

19 *In the Matter of ACRAnet, Inc.*, Docket No. C-4331, Complaint (Aug. 19, 2011) https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110809acranetcmpt.pdf, *archived at* https://perma.cc/SUZ8-N78E; *In the Matter of Fajilan and Associates, Inc.*, Docket No. C-4332, Complaint (Aug. 19, 2011) https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819statewidecmpt.pdf, *archived at* https://perma.cc/D83U-STTY.

20 Materials in the Henry Schein proceeding are available at https://www.ftc.gov/enforcement/cases-proceedings/142-3161/henry-schein-practice-solutions-inc-matter, *archived at* https://perma.cc/4HMH-5BR3.

The case illustrates the FTC's view that a software maker can be held liable for making deceptive statements about data security to its business customers, even if the statements are not made to the individuals whose personal information is put at risk. For other software or devices cases, see Chapter 6.1.

10.4.2.5 Failure to Respond to Vulnerability Reports

In February 2016, the FTC announced its settlement with ASUSTek, which makes routers.[21] The FTC alleged that the company had misrepresented its security practices and failed to properly design or test its router software. For example, the company set the default login credentials as username "admin" and password "admin" and allowed consumers to retain those credentials. One thing notable about the proceeding is that the commission cited the company's failure to address vulnerability reports as one of its primary concerns. The vulnerability reports came from consumers, security researchers, and the media. The proceeding indicates that a software or device maker must respond promptly when security vulnerabilities come to its attention though any reliable channel.[22]

10.4.3 The FTC Survives Judicial Challenges to its Section 5 Authority

Most companies that come within the FTC's cybersecurity enforcement crosshairs settle. However, three companies resisted. In the first case, *Wyndham*, the Third Circuit in 2015 affirmed the FTC's authority over data security under Section 5 and it upheld the FTC's case-by-case approach to defining unreasonable security. In the second, a federal district court similarly rejected an argument that the FTC's unfairness

21 Materials in the ASUSTek proceeding are available at https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter, *archived at* https://perma.cc/59SD-TDZN.

22 Other cases where the FTC alleged that the failure to maintain an adequate process for receiving and addressing security vulnerability reports from security researchers and academics is an unreasonable practice, in violation of Section 5: *In the Matter of HTC America*, FTC No. 1223049, Complaint (July 2, 2013), https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter; and *In the Matter of TRENDnet, Inc*. FTC No. 1223090, Complaint, (Feb. 7, 2014) https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter, *archived at* https://perma.cc/S8HY-Y4XY.

authority did not extend to general data security practices, but it raised questions about the FTC's definition of injury. The third, *LabMD*, also questioned the FTC's view on injury and, in a decision handed down by the Eleventh Circuit in 2018, temporarily cast doubt on the FTC's overall strategy. In 2019, however, the FTC recovered and reasserted itself, adding much greater specificity to its cybersecurity orders.

10.4.3.1 *Wyndham*: Weak Cybersecurity Can Be "Unfair"

Wyndham Worldwide manages and franchises hotels located around the world. As part of its normal business in accepting payments, the company collects personal and financial information from customers, including credit card information. Three times between 2008 and 2009, hackers invaded Wyndham's computer network, stealing information for more than 619,000 Wyndham customers, primarily credit card information, resulting in at least $10.6 million in fraud loss. In June 2012, after an extensive investigation, the FTC filed a district court complaint against Wyndham.

According to the FTC, Wyndham:

- Failed to use firewalls at critical network points.
- Stored payment card information in cleartext.
- Failed to ensure that branded hotels implemented adequate policies and procedures.
- Failed to remedy known security vulnerabilities.
- Allowed use of default user names and passwords.
- Allowed use of easily guessed passwords.
- Failed to inventory connected devices.
- Failed to use intrusion detection measures.
- Failed to monitor for malware.
- Failed to restrict third-party vendors' access to the Wyndham network.

Unlike Eli Lilly, Wyndham did not settle. Instead, it challenged the authority of the FTC to regulate cybersecurity, raising a variety of arguments.

In 2015, the Third Circuit issued a landmark decision in which it upheld the FTC's authority to use the unfairness prong of its Section 5 authority as the basis of cybersecurity enforcement. *FTC v. Wyndham Worldwide Corporation,* 799 F.3d 236 (3d Cir. 2015). The court rejected each of Wyndham's arguments, holding that:

- Conduct does not have to be unscrupulous or unethical to be unfair under Section 5.
- Wyndham was not spared liability because it was a victim of a cyberattack.
- Unfairness claims may be brought on the basis of likely rather than actual injury, 799 F.3d at 246.
- More tailored cybersecurity statutes (the FCRA, GLBA, and COPPA) did not deprive FTC of authority.

Most significantly, perhaps, the court held that Wyndham had not been denied adequate notice of the specific cybersecurity standards that it was required to follow. The Third Circuit held that Wyndham received all the notice it was entitled to: fair notice that its conduct could fall within the meaning of the statute, given the cost-benefit analysis required under Subsection (n). This did not mean that Wyndham was entitled to notice of what specific cybersecurity practices are necessary to avoid liability. The court noted that the complaint alleged Wyndham's complete failure to provide any form of security with respect to key items (firewalls, encryption, passwords). The court noted that the company had been breached three times so it should have known that a court might find its practices failing a cost-benefit analysis. Other considerations: The FTC's published guidance had counseled against many of the practices Wyndham engaged in, and the prior enforcement actions of the FTC "help[ed] companies with similar practices apprehend the possibility that their cybersecurity practices could fail [the cost-benefit analysis of 5(n)] as well."

In December 2015, after the Third Circuit's ruling, Wyndham accepted a stipulated order for injunction in which it agreed to establish and maintain for 20 years a comprehensive cybersecurity program that was very similar to the one imposed on Eli Lilly a decade earlier. The FTC added one new element: Obtain, for 20 years, an annual,

independent assessment of compliance with the Data Security Standard of the payment card industry. Other than that, the FTC's remedies against Wyndham tracked those of Eli Lilly and the GLBA Safeguards Rule, 13 years earlier.

10.4.3.2 *D-Link*: Questioning the FTC's Interpretation of "Injury"

D-Link sells routers and IP cameras. It marketed these products as providing good data security because they featured "the latest wireless security features to help prevent unauthorized access" and "the best possible encryption" protections, among other safeguards. The FTC brought a complaint in federal court alleging that, in fact, D-Link failed to protect its products from "widely known and reasonably foreseeable risks of unauthorized access" by not providing "easily preventable" measures against "'hard-coded' user credentials and other backdoors"; not maintaining the confidentiality of the private key D-Link used with consumers to validate software updates; and not deploying "free software, available since at least 2008, to secure users' mobile app login credentials." As a consequence, "consumers' sensitive personal information and local networks" were at significant risk of being accessed by unauthorized agents. The FTC alleged that D-Link's practices were unfair and deceptive.

D-Link moved to dismiss the complaint. As a preliminary matter, the court held that FTC deception claims must satisfy the specificity requirements of Rule 9(b). *FTC v. D-Link Sys.,* Case No. 3:17-cv-00039-JD, 2017 U.S. Dist. LEXIS 152319 (N.D. Ca. Sept. 19, 2017). The court held that three of the FTC's five deception claims had been adequately pleaded. Two of the claims were dismissed with leave to amend.

On unfairness, D-Link argued that the unfairness prong of Section 5 did not give the FTC authority over general data security practices. The court rejected this argument, stating, "Congress intentionally made Section 5 open-ended, and explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply." Id at *10-11. "Consequently, the fact that data security is not expressly enumerated as within the FTC's enforcement powers is of no moment to the exercise of its statutory authority." *Id.* at *11. The court also rejected D-Link's argument that fair notice requires

that the FTC adopt standards before pursuing enforcement actions: "to require the FTC in all cases to adopt rules or standards before responding to data security issues faced by consumers is impractical and inconsistent with governing law." *Id*. at *12.

However, the court found that the FTC's unfairness allegation did not satisfy Subsection 5(n), which bars the FTC from declaring an act or practice unfair unless it "causes or is likely to cause substantial injury to consumers." The court stated, "The FTC does not allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed. Instead, the FTC relies solely on the likelihood that [D-Link] put consumers at 'risk'" because remote attackers could exploit its devices through their widely known vulnerabilities. *Id.* at *14. "[T]he FTC cannot rely on wholly conclusory allegations about potential injury to tilt the balance in its favor." *Id*. at *15. The court pointed the FTC toward a possible approach: "If the FTC had tied the unfairness claim to the representations underlying the deception claims, it might have had a more colorable injury element. A consumer's purchase of a device that fails to be reasonably secure—let alone as secure as advertised—would likely be in the ballpark of a 'substantial injury,' particularly when aggregated across a large group of consumers." *Id*. at *16.

As it happened, the FTC did not file an amended complaint. Based on the deception claims alone, D-Link settled.[23]

10.4.3.3 *LabMD*: More Questions About "Substantial Injury"

In 2009, a cybersecurity research firm discovered that that files from a small company called LabMD were publicly available through the LimeWire peer-to-peer filing-sharing app. It appeared that a LabMD employee had loaded the app on a work computer in order to access music, but LimeWire exposed other contents of the employee's computer, including a file with the personal information of 9,300 consumers. After a lengthy proceeding, the FTC filed an administrative complaint alleging that "LabMD's security practices were unreasonable, lacking even basic precautions to protect the sensitive consumer information maintained

23 *FTC v. D-Link Systems, Inc.*, No. No. 3:17-cv-00039-JD, Stipulated Order for Injunction and Judgment (July 2, 2019) https://www.ftc.gov/system/files/documents/cases/dlink_proposed_order_and_judgment_7-2-19.pdf, *archived at* https://perma.cc/5NR9-KRTM.

on its computer system. Among other things, it failed to use an intrusion detection system or file integrity monitoring; neglected to monitor traffic coming across its firewalls; provided essentially no data security training to its employees; and never deleted any of the consumer data it had collected."[24] (Note how far the findings went beyond the careless installation of the P2P software.)

The case required the commission to squarely face the question of what constituted harm for purposes of Subsection 5(n), which prohibits the commission from acting unless the act or practice at issue "causes or is likely to cause substantial injury to consumers." Although there was no evidence of ID theft or economic or physical harm due to exposure of the information, which may have been seen only by the security research firm that discovered the problem and brought it to the FTC's attention, the FTC concluded that "the disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n)." Independently, the commission concluded, the unauthorized disclosure of medical data was likely to cause substantial injury in the form of medical ID theft. The commission said that showing a "significant risk" of injury satisfies the "likely to cause" standard.[25]

LabMD appealed to the Eleventh Circuit. In a preliminary ruling, the court granted a stay of the FTC's order after finding "there are compelling reasons why the FTC's interpretation [of its authorities] may not be reasonable." *LabMD v. FTC,* 678 F. App'x 816 (11th Cir. 2016). Specifically, the court concluded that "it is not clear that a reasonable interpretation of § 45(n) includes intangible harms like those that the FTC found in this case." 678 F. App'x at 820. Second, the court rejected the FTC's interpretation of "likely to cause" as that term is used in § 45(n). The FTC had interpreted "likely to cause" to mean "significant risk" and had concluded that "a practice may be unfair if the magnitude

24 *In the Matter of LabMD, Inc.,* Complaint (Aug. 29,2013) https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf, *archived at* https://perma.cc/MR4Y-6S25.

25 *In the Matter of LabMD, Inc.,* Opinion of the Commission (July 29, 2016) https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf, *archived at* https://perma.cc/HYF4-SVW7. See also *In the Matter of LabMD, Inc.,* Final Order (July 9, 2016) https://www.ftc.gov/system/files/documents/cases/160729labmdorder.pdf, *archived at* https://perma.cc/VK5T-LH8J.

of the potential injury is large, even if likelihood of the injury occurring is low." The court disagreed: "We do not believe an interpretation that does this is reasonable." *Id.* at 821.

Despite the rulings in *D-Link* and *LabMD*, the FTC has continued to allege substantial injury where no data was compromised or where it was exposed but not misused. In its case against Zoom, for example, the commission alleged that Zoom's circumvention of a privacy and security safeguard in the Safari browser harmed consumers by limiting the intended benefit of the safeguard and by introducing two additional security vulnerabilities, although the exploitation of those flaws was only hypothetical.[26] In a case against SkyMed International, the FTC alleged that the failure to provide reasonable security for consumers' personal information "has caused or is likely to cause substantial injury to those consumers." There, an unsecured cloud database containing more than 130,000 records of consumers' personal information, including medical data, was publicly available on the internet for at least five months, but there was no allegation that the data was viewed by anyone other than the independent security researcher who discovered it.[27]

10.4.3.4 *LabMD*: Reasonableness Is Unreasonable

When it reached the merits, the Eleventh Circuit faced an FTC order against LabMD that followed the template established in *Eli Lilly* and *BJs*':

Eli Lilly (2002)	LabMD (2016)
Establish and maintain info security program.	Establish and maintain comprehensive written information security program with appropriate administrative, technical, and physical safeguards *reasonably designed* to protect.
Designate personnel to coordinate.	Designate employee(s) to coordinate and be accountable.

26 *In the Matter of Zoom Video Communications, Inc.*, Complaint (Nov. 9, 2020) https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf, archived at https://perma.cc/LS7J-N4EN.

27 *In the Matter of SkyMed International, Inc.*, Complaint (Dec. 16, 2020) https://www.ftc.gov/system/files/documents/cases/skymed_-_complaint.pdf, *archived at* https://perma.cc/4DEU-N4DZ.

Identify reasonably foreseeable risks.	Identify material risks, including training, info systems, incident prevention, and response.
Address risks identified, including training, info systems, incident prevention and response.	Design & implement *reasonable* safeguards to control risks identified.
	Regularly test or monitor.
Conduct annual written review by qualified persons to monitor and document compliance.	Obtain biennial assessment from qualified, objective, independent third-party professional.
"Whether by employees or agents."	Take *reasonable steps* to select and retain service providers capable of safeguarding personal info.
Evaluate effectiveness and adjust.	Evaluate and adjust.
	Notice to affected customers.
Order remains in effect 20 years.	Order remains in effect 20 years

The Eleventh Circuit said that the first question presented by the appeal was "whether LabMD's failure to implement and maintain a reasonably designed data-security program constituted an unfair act or practice within the ambit of Section 5(a)." *LabMD, Inc. v. FTC,* 894 F.3d 1221, 1230 (11th Cir. 2018). On this point, the court's ruling is not dispositive: "We will assume *arguendo* that the Commission is correct and that LabMD's negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice." The path the court took to get to that point is questionable: Relying on a 1964 FTC policy statement and a 1980 commission letter to Congress, the court concluded that "[t]he Commission must find the standards of unfairness it enforces in 'clear and well-established' policies that are expressed in the Constitution, statutes, or the common law." *Id*. at 1231.

However, the 1980 letter expressly contradicts this, stating, "Unjustified consumer injury is the primary focus of the FTC Act . . . . By itself it can be sufficient to warrant a finding of unfairness."[28] In addition, it would seem

28 *FTC Policy Statement on Unfairness* (Dec. 17, 1980) https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness*, archived at* https://perma.cc/C8EM-3BPX.

that both the 1964 policy and the 1980 letter had been superseded or at least affected by Subsection 5(n) of the FTC Act, which was adopted in 1994. Subsection 5(n) states, "In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination." This is quite the opposite of saying that the commission must find a violation of public policy. The Eleventh Circuit's only reference to this legislative language was in a footnote, where the court called it an "ambiguous statement." In any event, the Appeals Court went on the find that the FTC's source of "clear and well-established" policies in the cybersecurity realm was the common law of negligence. *Id.* at 1231.

On the question of harm, which had been central to the proceedings below, the court said little, although it suggested that an exposure of data causes injury that the commission can address: "The complaint then alleges that LimeWire's installation caused the 1718 File, which consisted of consumers' personal information, to be exposed. The 1718 File's exposure caused consumers injury by infringing upon their right of privacy. Thus, the complaint alleges that LimeWire was installed in defiance of LabMD policy and caused the alleged consumer injury. Had the complaint stopped there, a narrowly drawn and easily enforceable order might have followed, commanding LabMD to eliminate the possibility that employees could install unauthorized programs on their computers." *Id.* at 1229.

The court then turned to the second question presented on appeal: whether the commission's cease-and-desist order, founded upon LabMD's general negligent failure to act, was enforceable. On this, the court was clear: "We answer this question in the negative." The FTC order was unenforceable because "[i]t does not enjoin a specific act or practice." Zeroing in on the word "reasonable," the court said that the FTC order was "devoid of any meaningful standard informing the court of what constitutes a 'reasonably designed' data-security program."

> In sum, assuming arguendo that LabMD's negligent failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a), the Commission's cease and desist order is nonetheless unenforceable. It does not enjoin a specific act or practice.

> Instead, it mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished. Moreover, it effectually charges the district court with managing the overhaul. This is a scheme Congress could not have envisioned. We therefore grant LabMD's petition for review and vacate the Commission's order. 894 F.3d at 1237.

But *LabMD* did not end the FTC's cybersecurity enforcement activity. Instead, it prompted a fundamental shift in the FTC's approach, to very highly detailed orders, loaded with technical measures.

10.4.4 Section 5 After *LabMD*—More Detailed Orders

The Eleventh Circuit's decision looked at first like a fatal blow, but on closer examination, the court's fixation on "reasonableness" and its criticism that the FTC's order was too open-ended pointed to a solution.

10.4.4.1 *Lightyear*

The FTC's new approach was first displayed in a case against Lightyear, which develops and sells management software and data processing services to auto dealerships. Lightyear's software tracks information related to all aspects of a dealership's business: sales, finance, inventory, accounting, payroll, customer management, and parts and service. Lightyear stores the information on its network, either for processing or as backup, comprising personal information on about 14 million dealership customers and about 39,000 dealership employees.

According to the FTC, Lightyear stored all the information in plain text. In about April 2015, Lightyear directed an employee to purchase an additional storage device and attach it to the company network. At no time, according to the FTC, did any manager provide the employee with any guidance or take any steps to ensure the new storage device was securely configured. The device created an open connection port which a hacker found and exploited, downloading information on 69,283 consumers. The FTC opened an investigation and filed a complaint. It alleged that Lightyear failed to provide reasonable security for the personal information stored on its network. Among other things, the respondent:

a. Failed to develop, implement, or maintain a written organizational information security policy.

b. Failed to implement reasonable guidance or training for employees or third-party contractors, regarding data security and safeguarding consumers' personal information.

c. Failed to assess the risks to the personal information stored on its network, such as by conducting periodic risk assessments or performing vulnerability and penetration testing of the network.

d. Failed to use readily available security measures to monitor its systems and assets at discrete intervals to identify data security events (e.g., unauthorized attempts to exfiltrate consumers' personal information across the company's network) and verify the effectiveness of protective measures.

e. Failed to impose reasonable data access controls, such as restricting inbound connections to known IP addresses, and requiring authentication to access backup databases.

f. Stored consumers' personal information on the respondent's computer network in clear text.

g. Failed to have a reasonable process to select, install, secure, and inventory devices with access to personal information.

The complaint alleged that the failure to employ reasonable measures was an unfair act or practice. The complaint separately alleged violation of the GLBA Safeguards Rule, since Lightyear fit within the broad definition of a financial institution.

Lightyear settled. Like Eli Lilly and most other respondents, it agreed to establish a comprehensive information security program to protect consumer information. But in key respects, the consent order differed from all prior orders: It struck the word "reasonable," and it added substantial specific details:

BJ's (2005)	Lightyear (2019)
Establish, implement and maintain comprehensive written info security program reasonably designed to protect personal info, with appropriate administrative, technical, and physical safeguards.	Establish and maintain comp. written info sec program that protects personal info.

	Provide program and evaluations to board.
Designate employee(s) to coordinate and be accountable.	Designate qualified employee(s) to coordinate and be accountable.
Identify material internal and external risks—training, info systems, and prevention, detection and response.	Assess and document at least once every 12 months internal and external risks.
Design and implement reasonable safeguards to control risks identified.	Design, implement, maintain, and document safeguards to control risks identified.
	Training all employees at least once every 12 months.
Regularly test or monitor effectiveness.	Monitor all networks, systems, and assets to identify security events, including exfiltration.
	Restrict inbound IP connections; require authentication; limit access by function.
	Encrypt Social Security numbers and financial account info.
	Ensure secure installation and inventory of devices.
	Assess sufficiency at least once a year and promptly following any security incident.
	Test and monitor effectiveness at least once every 12 months.
	Vulnerability testing once every four months.
Obtain assessment from qualified, objective, independent third-party professional every two years.	Obtain biennial assessment from qualified, objective, independent third-party professional.
	Select and retain service providers capable of safeguarding personal info.
Evaluate and adjust.	Evaluate and adjust.
	Notice to FTC of all breaches.
Order remains in effect 20 years.	Order remains in effect 20 years.

In addition to its lack of the reasonableness standard that the Eleventh Circuit had objected to and the obviously greater level of depth of its requirements, the order is also notable for the relatively close fit between the failings that were alleged and the remedies that were ordered.

10.4.4.2 *Equifax*

As noted, the Equifax breach was massive and especially worrisome because Equifax maintained the data elements that are the building blocks of ID theft. Ultimately, the DOJ indicted Chinese military officers for the attack.[29] The fact that the attack was state-sponsored did not spare Equifax from FTC enforcement. The FTC's 2019 complaint and settlement against Equifax is a good, if extreme, illustration of the post-*LabMD* reality. The complaint alleges that Equifax failed to provide reasonable security for the massive quantities of sensitive personal information stored within its computer network. Among other things:

> A. Defendant failed to implement reasonable procedures to detect, respond to, and timely correct critical and other high-risk security vulnerabilities across Defendant's systems, including:
>
> > i. Patch management policies and procedures that failed to ensure the timely remediation of critical security vulnerabilities;
> >
> > ii. Widespread noncompliance with Defendant's patch management policy, including unpatched critical and high-risk vulnerabilities across Defendant's systems that persisted for months;
> >
> > iii. A failure to implement reasonable intrusion protection controls in legacy systems; including:
> >
> > > a) Failures to implement host and network intrusion prevention or file integrity monitoring that could have identified unauthorized access to Defendant's network; and

29 U.S. Department of Justice, Office of Public Affairs, *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax* (Feb. 10, 2020) https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking, *archived at* https://perma.cc/32X9-AHL6.

b) Failures to maintain security certificates that would have allowed Defendant to examine traffic for suspicious activity;

iv. Failures to implement readily-available protections, including many low-cost protections, against well-known and reasonably foreseeable vulnerabilities, such as CrossSite Scripting ("XSS"), Structured Query Language ("SQL") injection, security misconfigurations, and other common vulnerabilities, that could be exploited to gain unauthorized access to sensitive personal information and local networks;

B. Defendant failed to use readily available security measures to segment its servers and databases;

C. Defendant failed to implement or enforce reasonable access controls to prevent unauthorized access to sensitive personal information. For example,

i. Defendant stored numerous administrative credentials with access to sensitive personal information in plain text;

ii. Defendant copied sensitive personal information, including SSNs, to numerous systems for development and testing purposes, which were accessible by employees and contractors without any business need;

iii. Defendant failed to monitor or log privileged account activity across numerous systems; and

iv. Until at least 2017, Defendant failed to limit administrative rights for any of its employees on company-issued PCs and other devices, and allowed users to install any software or alter configurations;

D. Defendant stored sensitive personal information in plain text, including hundreds of millions of SSNs and payment card information, including credit card account numbers provided by consumers to purchase direct-to-consumer products; and

E. Defendant failed to provide adequate security training for engineers and other employees.

The FTC's settlement order is equally detailed. It imposed not only the procedural requirements of its earlier orders (implement and maintain a comprehensive information security program, designate an employee to be responsible for the program, assess risks and adopt safeguards to respond to them, monitor regularly, vet vendors and bind them contractually to implement safeguards, third party assessments) but also a long list of additional, quite specific safeguards. The order specifies that such safeguards *shall* include:

- Establish patch management procedures that require confirmation that patches are completed.
- Enforce policies to ensure timely remediation of critical or high-risk vulnerabilities.
- Document a comprehensive IT asset inventory.
- Design and implement protections, such as intrusion protection and file integrity monitoring.
- Implement measures to limit unauthorized access, such as segmentation and properly configured firewalls.
- Implement access controls, such as multi-factor authentication and strong passwords.
- Limit user access privileges to those with a business need to access.
- Implement protections, such as encryption, or alternative compensating controls, for information in transit and at rest.
- Establish and enforce procedures to ensure use of secure development practices for applications developed in-house.
- Evaluate, assess, or test the security of externally developed apps.
- Regular training.
- Establish an easily accessible process for receiving and addressing vulnerability reports from third parties.
- Establish a process for employee complaints or concerns about information security.

- Vulnerability testing of its network at least once every four months.

Plus $300 million in monetary relief, with the possibility of $125 million more (up to $700 million total counting settlements with the states).

10.4.4.3 *Zoom*

As of February 15, 2021, the most recent major cybersecurity case settled by the FTC was against Zoom.[30] In some respects, it was a typical deception case: The FTC alleged that Zoom made statements about encryption of users' meetings that were not true. The FTC also alleged deception by omission: Failing to tell users that an update to its Mac app would circumvent a Safari browser privacy and security safeguard.

In settlement, Zoom agreed to terms similar to those in other recent cases.[31] Without admitting or denying any of the FTC's allegations, Zoom agreed to establish and implement a comprehensive information security program; assess and document on an annual basis any internal and external data security risks; implement safeguards against such risks; implement other specific measures, including review all software updates for security flaws; ensure the updates will not hamper third-party security features; implement a vulnerability management program; institute data deletion controls; take steps to prevent the use of known compromised user credentials and credential stuffing; and deploy safeguards "such as" multi-factor authentication to protect against unauthorized access to its network. And the company must obtain biennial assessments of its security program by an independent third party, which the FTC has authority to approve, and notify the commission if it experiences a data breach.

In three ways, however, the case was especially noteworthy: First was the fact that the FTC acted before a data breach had occurred. Second was the FTC's assertion that limiting the intended benefit of a privacy

30 *In the Matter of Zoom Video Communications, Inc.,* Complaint (Nov. 9, 2020) https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf.

31 *In the Matter of Zoom Video Communications, Inc.,* Agreement Containing Consent Order (Nov. 9, 2020) https://www.ftc.gov/system/files/documents/cases/1923167zoomacco2.pdf.

and security safeguard was itself a substantial injury to consumers, giving rise to liability under Section 5.

Third were the dissents by Commissioners Rebecca Kelly Slaughter and Rohit Chopra. Slaughter criticized the commission for treating privacy and security as separate issues.[32] She argued that the FTC should have required Zoom to engage in a review of the risks to consumer *privacy* presented by its products and services, implement procedures to routinely review such risks, and build in privacy-risk mitigation before implementing any new or modified product, service, or practice. She also argued that the settlement was deficient because it included no redress or recourse for customers adversely affected by Zoom's deception.

Chopra offered specific recommendations: Strengthen orders to emphasize more help for individual consumers and small businesses; comprehensively investigate data protection, consumer protection, and competition; diversify the FTC's investigative teams to increase technical rigor; consider restating its cybersecurity precedent into a rule under Section 18 or other appropriate statutes to provide clear guidance and systematically deter unlawful data protection practices; demonstrate greater willingness to pursue administrative and federal court litigation; increase cooperation with international, federal, and state partners; and determine whether third-party assessments are effective.[33]

In January 2021, Slaughter became acting chair of the FTC. She will, after President Biden's nominations are confirmed, become part of a Democratic majority on the FTC. Meanwhile, the president nominated Chopra to head the CFPB, and it is unclear whether the new Democratic majority of the FTC will take up his recommendations.

See Chapter 10.4.8 below for what to make of all this.

32 *In the Matter of Zoom Video Communications, Inc.*, Dissenting Statement of Commissioner Rebecca Kelly Slaughter (Nov. 9, 2020) https://www.ftc.gov/system/files/documents/public_statements/1582918/1923167zoomslaughterstatement.pdf.

33 *Dissenting Statement of Commissioner Rohit Chopra Regarding Zoom Video Communications, Inc.* (Nov. 6, 2020 https://www.ftc.gov/system/files/documents/public_statements/1582914/final_commissioner_chopra_dissenting_statement_on_zoom.pdf.

10.4.5 Fines and Penalties

"The FTC generally cannot seek civil penalties for initial violations of the FTC Act, but if a company violates an FTC order, the FTC can seek civil monetary penalties for the violations, as it did last year when it announced a $5 billion settlement with Facebook."[34] Such an action is brought in district court by the attorney general, in the name of the U.S., under Section 5(l) of the FTC Act. 15 U.S.C. § 45(l).[35]

Section 13(b) of the FTC Act authorizes the commission to bring suit in federal court to enjoin any violation of any provision of law enforced by the FTC. 15 U.S.C. § 53(b). In filing such complaint, the FTC used to ask the courts, in the exercise of their equitable jurisdiction, to award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC. That is what the commission did in its case against Equifax, resulting in a settlement under which Equifax was required to pay $300 million to a fund to provide affected consumers with credit monitoring services and to compensate consumers who bought credit or identity monitoring services from Equifax and paid other out-of-pocket expenses as a result of the data breach.

However, in April 2021, the Supreme Court brought this practice to an abrupt and conclusive end when it ruled unanimously that Section 13(b) does not authorize the FTC to seek, or a court to award, equitable monetary relief such as restitution or disgorgement. *AMG Capital Management LLC v. FTC,* 2021 U.S. LEXIS 2108 (Apr. 22, 2021).

The commission has a third avenue, rarely used, under Section 19 of the FTC Act, 15 U.S.C. § 57b: If any person engages in any unfair or deceptive act or practice with respect to which the commission has issued a final cease-and-desist order that is applicable to such person, the commission may commence a civil action against such person in a

34 FTC, *FTC's Use of Its Authorities to Protect Consumer Privacy and Securit*y (2020) at https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf*, archived at* https://perma.cc/XU6T-8LAV.

35 See *U.S. v Facebook,* Case No. 19-cv-2184, Complaint for Civil Penalties, Injunction, and Other Relief (D. D.C. July 24, 2019) https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf, *archived at* https://perma.cc/CJA4-Z2UV.

U.S. district court or in any court of competent jurisdiction of a state. If the commission satisfies the court that the act or practice to which the cease-and-desist order relates is one that a reasonable man would have known under the circumstances was dishonest or fraudulent, the court may grant such relief as the court finds necessary to redress injury to consumers or other persons, including rescission or reformation of contracts, the refund of money or return of property, and the payment of damages.

10.4.6 GLBA Enforcement

Let's not forget GLBA. The definition of financial institution is very broad. 15 U.S.C. § 6809(3)(A), 16 C.F.R. § 313.1(b). In some of its enforcement actions, the FTC has cited both Section 5 and GLBA. (A notable example: the case against Equifax for its enormous breach.) In others, it has proceeded purely under GLBA. A recent example of the latter is the 2020 case against Ascension Data & Analytics, LLC, a company that provides data, analytics, and technology services and products in connection with mortgages, including the storing and organizing of mortgage documents. Ascension hired an unaffiliated company to process mortgage documents which contained Social Security numbers, loan information, credit and debit account numbers, drivers' license numbers, credit files, or other personal and financial information of borrowers. The third party stored the documents on misconfigured cloud resources, leaving the sensitive personal information of tens of thousands of consumers exposed to anyone on the internet. The FTC alleged that Ascension violated the GLBA Safeguard Rule provision requiring that a regulated entity oversee its service providers. In particular, the FTC alleged, Ascension failed to take any formal steps to evaluate whether service providers could reasonably protect the personal information entrusted to them and failed to require service providers by contract to implement appropriate safeguards for personal information that the respondent provided to those service providers.[36]

36 *In the Matter of Ascension Data & Analytics*, LLC, Complaint and Agreement Containing Consent Order (Dec. 15, 2020) https://www.ftc.gov/enforcement/cases-proceedings/192-3126/ascension-data-analytics-llc-matter, *archived at* https://perma.cc/K7SR-RU93.

10.4.7 GLBA Safeguards: The Next Generation

In March 2019, with two commissioners dissenting, the FTC announced that it was seeking comment on proposed amendments to the GLBA Safeguards Rule.[37] The proposal would amend the rule to include more specific security requirements. Concluding that "a checklist approach is not appropriate" and that "very specific requirements for information security programs could become outdated and require frequent amendments," the commission stated that "the proposed amendments provide more detailed requirements as to the issues and threats that must be addressed by the information security program, but do not require specific solutions to those problems. Instead, the proposed amendments retain the process-based approach of the Rule, while providing a more detailed map of what information security plans must address."

Despite that caveat, the proposed amendments were very detailed indeed. Among other things, the revisions would require covered entities to:

- Articulate criteria for the evaluation and categorization of identified security risks or threats.
- Identify all data, personnel, devices, systems, and facilities.
- Place access controls on information systems, including controls to authenticate users and permit access only to authorized individuals.
- Protect by encryption all customer information in transit over external networks and at rest, or, if encryption is deemed infeasible, use instead effective alternative compensating controls.
- Adopt secure development practices for in-house developed apps and procedures for evaluating, assessing, or testing the security of externally developed apps.

37 The Notice of Proposed Rulemaking was officially published in the Federal Register on April 4, 2019. FTC, *Standards for Safeguarding Customer Information—Notice of Proposed Rulemaking,* 84 Fed. Reg. 13158 (Apr. 4, 2019) https://www.govinfo.gov/content/pkg/FR-2019-04-04/pdf/2019-04981.pdf, *archived at* https://perma.cc/H636-RUGH, and https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information, *archived at* https://perma.cc/9F3E-Y2KH.

- Implement multi-factor authentication for any individual accessing customer information.
- Include audit trails designed to detect and respond to security events.
- Develop, implement, and maintain procedures for the secure disposal of customer information.
- Adopt procedures for change management.
- Implement policies, procedures, and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.
- Conduct continuous monitoring or periodic penetration testing and vulnerability assessments.
- Verify that key information security personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

In many ways, the proposed rule would align GLBA safeguards with the more detailed orders seen in *Lightyear, Equifax* and other recent cases. In July 2020, the FTC held a workshop on issues raised in response to the proposed amendments. The FTC extended until August 12, 2020, the deadline for filing comments on the topics discussed at the workshop. Watch for further action by the commission. Time will tell whether industry manages to water down the provisions.

10.4.8 What Does the FTC Expect Under Section 5?

In a seminal 2014 article, Dan Solove and Woodrow Hartzog demonstrated that the FTC complaints, orders, and settlements constitute a common law of privacy and cybersecurity.[38] This is not a common law of findings let alone one of articulated reasoning. It is a common law *implied* from allegations and remedies. Through its complaints, the FTC has identified a list of what it alleges are unreasonable—and therefore unfair and therefore illegal—practices. Through its orders and settlements, the commission

38 Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L.Rev. 583 (2014).

has articulated a set of practices that would remedy the illegal state of the respondent and that, therefore, constitute a reasonable security program.

For example, in its complaint against the Wyndham hotel chain, the FTC alleged that the company failed to provide reasonable and appropriate security for the personal information it collected by, "[a]mong other things," failing to use firewalls, failing to remedy known security vulnerabilities, and failing to require complex passwords. If these failings constitute unreasonable security, doing their opposite would seem to be required in order to practice reasonable security. In its Equifax order, the FTC required the company to adopt a comprehensive information security program and also to implement a number of specific measures, including establishing patch management procedures that require confirmation that patches are completed; enforcing policies to ensure timely remediation of critical or high-risk vulnerabilities; documenting a comprehensive IT asset inventory; designing and implementing protections, such as intrusion protection and file integrity monitoring; and implementing measures to limit unauthorized access, such as segmentation and properly configured firewalls. Implicitly, these measures are part of a cybersecurity program that is not unfair.

As a means of defining cybersecurity obligations for all entities under the FTC's jurisdiction, this approach always had a flaw: The detailed allegations of unreasonableness in the FTC's complaints, if taken individually and cumulated, required too much while the settlements or orders through *LabMD* required too little. This is a flaw inherent in the case-by-case approach in which everything ends in a settlement without an admission of wrongdoing and without an adjudication of unfairness. On the allegations side, the FTC never said that any one failing alleged in its complaints was, by itself, unfair in all cases for all entities. Instead, the typical FTC compliant identifies multiple failings and then alleges that those failings taken together are evidence of a failure by that respondent to employ reasonable and appropriate measures and that that failure, based on all the failings taken together, is *an* unfair act or practice. Nor has the FTC ever given assurance that, if an entity avoided all of the specific failings identified in all of its complaints that it would be home free. A never-previously alleged failing could still, in the next case, be cited as an unfair act or practice.

The same can be said of its orders and settlements. At least from the *Eli Lilly* case in 2002 through its *LabMD* decision in 2016, the commission required parties to establish comprehensive information security programs, with safeguards to control the risks identified through a risk assessment. The elements of the settlements were very similar to those in the commission's GLBA rule, while carefully refraining (just as in the GLBA rule) from dictating specific procedures or technologies. Presumably, the settlements and orders through the *LabMD* case did contain the irreducible minimum of reasonable security, a conclusion bolstered by their similarity to the GLBA rule. But the items in the settlements and orders before *LabMD* were clearly never enough to constitute adequate security. Before 2019, the FTC never required encryption of wireless transmissions or prompt patching, but it seems impossible that a program lacking those measures would be considered adequate. After *LabMD*, the problem still exists: Even if a company did everything required of Equifax or even everything required of every company in every settlement and order, it might still be alleged to be engaged in unfair acts or practices based on some other flaw.

How to square the circle? The answer, highly unsatisfying but nevertheless probably all we have, lies in the commission's totality of the circumstances approach. As the Third Circuit said in the Wyndham case, "[T]he relevant inquiry here is a cost-benefit analysis." *FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 236, 255 (3d Cir. 2015). The commission has made it clear that there is no one-size-fits-all approach to cybersecurity.[39] It has stressed that a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. And it must be regularly revised in light of the changing threat environment and changing security technologies and practices.

A tipoff to the FTC's approach is found in the Equifax settlement. The settlement states, "Each safeguard shall be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood, given the existence of other safeguards, that the risk could be realized and result in the unauthorized access, collection, use, alteration, destruction,

39 FTC, *Commission Statement Marking the FTC's 50th Data Security Settlement*, at 1 (Jan. 31, 2014).

or disclosure of the Personal Information." Further, the agreement refrains from actually requiring certain measures, Instead, it states that, to limit unauthorized access, Equifax must design, implement, and maintain measures, *such as* segmentation and properly configured firewalls, and it must implement access controls, *such as* multi-factor authentication. If encryption is infeasible, it must adopt effective alternative compensating controls. In other words, even within the detail of the Equifax settlement, the company is granted discretion to design its own security measures, based on the totality of the circumstances and a cost-benefit analysis.

The good and bad news is that each entity has to figure out what is best for its own situation. The commission's complaints constitute a list of practices that, in context, might be deemed illegal. And its settlements and orders constitute a list of measures that, thoughtfully assembled, will constitute reasonable security. Lawyers and senior IT staff for companies should go over the lists of alleged failings in recent cases and ask if their company is engaging in any of the practices cited in past complaints. Then, they should ask what would make sense for their company to address the deficiency. Starting with the *Lightyear*, *Equifax* and *Zoom* settlements, lawyers and senior IT staff for companies should determine what is feasible and appropriate, taking into account the nature and size of the business, the information it processes, the risks it faces, and so on, then document the rationale for not taking any particular action that would have addressed the failing identified in a complaint or a requirement imposed in a settlement. From a lawyering standpoint, the goal is to ensure that a client facing FTC investigation after a data spill can present a good reason for not doing something that the FTC had identified in a prior settlement.

The commission has made this process somewhat easier by compiling and summarizing its complaints through 2015, as explained in the next section.

10.4.9 FTC's Cybersecurity Allegations Translated into Security Best Practices

In 2015, the commission compiled the lessons of all of its cybersecurity enforcement actions to date into a guide for business,[40] organized thematically around a series of 10 cybersecurity practices:

- Start with security.
    - Don't collect personal information you don't need.
    - Hold onto information only as long as you have a legitimate business need.
    - Don't use personal information when it's not necessary.
- Control access to data sensibly.
    - Restrict access to sensitive data.
    - Limit administrative access.
- Require secure passwords and authentication.
    - Insist on complex and unique passwords.
    - Store passwords securely.
    - Guard against brute force attacks.
    - Protect against authentication bypass.
- Store sensitive personal information securely and protect it during transmission.
    - Keep sensitive information secure throughout its lifecycle.
    - Use industry-trusted and accepted methods.
    - Ensure proper configuration.

40 *Start with Security: A Guide for Business* (2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf, *archived at* https://perma.cc/T985-LRP6. The Commission has used its blog to give further guidance. Among the relevant entries: *Stick with Security* (2017) https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series, *archived at* https://perma.cc/WMS4-M2EM and *App Developers: Start with Security* (May 2017) https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security, *archived at* https://perma.cc/R747-W776.

- Segment your network and monitor who's trying to get in and out.
    - Segment your network.
    - Monitor activity on your network.
- Secure remote access to your network.
    - Ensure endpoint security.
    - Put sensible access limits in place.
- Apply sound security practices when developing new products.
    - Train your engineers in secure coding.
    - Follow platform guidelines for security.
    - Verify that privacy and security features work.
    - Test for common vulnerabilities.
- Make sure your service providers implement reasonable security measures.
    - Insist that appropriate security standards are part of your contracts.
    - Verify compliance.
- Put procedures in place to keep your security current and address vulnerabilities that may arise.
    - Update and patch third-party software.
    - Heed credible security warnings and move quickly to fix them.
- Secure paper, physical media, and devices.
    - Securely store sensitive files.
    - Protect devices that process personal information.
    - Keep safety standards in place when data is en route.
    - Dispose of sensitive data securely.

For example, the guide notes that, in a case against Twitter, the FTC had alleged that the company let employees use common dictionary

words as administrative passwords, as well as passwords they were already using for other accounts. Lesson learned: Insist on complex and unique passwords (subject to the cost-benefit analysis). In its case against Dave & Buster's, the FTC had alleged that the company didn't use an intrusion detection system or monitor system logs for suspicious activity. Lesson learned: Monitor activity on your network, subject to the cost-benefit analysis. In a 2017 blog, the FTC staff stated that, if there is one recurring theme running through its investigations that are ultimately closed *without* law enforcement action, it is that "those companies' practices often lined up with the common-sense security fundamentals in Start with Security."[41]

The FTC has a separate guide on IoT devices.[42]

41 Thomas B. Pahl, Acting Director, FTC Bureau of Consumer Protection, *Stick with Security: Insights into FTC Investigations* (July 21, 2017) https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations, *archived at* https://perma.cc/254C-TNQG.

42 FTC, *Careful Connections: Keeping the Internet of Things Secure* (Sept. 2020) https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-keeping-internet-things-secure, *archived at* https://perma.cc/Y5WA-HU7M.