No. 16-16270

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

LABMD, INC.,
Petitioner,

v.

FEDERAL TRADE COMMISSION,
Respondent.

On Petition for Review of an Order
of the Federal Trade Commission
(FTC Docket No. 9357)

BRIEF OF THE FEDERAL TRADE COMMISSION

DAVID C. SHONKA
Acting General Counsel

JOEL MARCUS
Deputy General Counsel

MATTHEW M. HOFFMAN
THEODORE (JACK) METZLER
Attorneys

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-3097
mhoffman@ftc.gov

Of Counsel:

LAURA RIPOSO VANDRUFF
ALAIN SHEER
JARAD BROWN

FEDERAL TRADE COMMISSION
Washington, D.C. 20580

CERTIFICATE OF INTERESTED PERSONS

Pursuant to Eleventh Circuit R. 26.1-1 to 26.15, the Federal Trade Commission certifies that the Certificate of Interested Parties in Petitioner LabMD's opening brief lists all trial judges, attorneys, persons, associations of persons, firms, partnerships, or corporations that had an interest in the outcome of this appeal as of the date it the brief was filed (December 27, 2016). Since then, several additional parties have appeared as *amici curiae* and the titles of two Commissioners have changed. Accordingly, the FTC supplements LabMD's Certificate of Interested Parties as follows:

Black, David L.—*Amicus Curiae*

Boies, Schiller & Flexner LLP—Counsel for *Amicus Curiae* NTSC

Cause of Action—Counsel for LabMD before FTC and counsel for *Amici Curiae* David Black *et al.*
(listed in LabMD's certificate solely as counsel for LabMD)

Chamber of Commerce of the United States of America—*Amicus Curiae*

Consovoy McCarthy Park PLLC—Counsel for *Amicus Curiae* Chamber of Commerce

Consovoy, William S.—Attorney, Consovoy McCarthy Park PLLC

Gilbert, Sheldon—Attorney—U.S. Chamber Litigation Center

Gottlieb, Michael J.—Attorney, Bois, Schiller & Flexner, LLP

Green,. Bruce G.—*Amicus Curiae*

Hader, Joan E.—*Amicus Curiae*

Hill, Brian E.—*Amicus Curiae*

Hitt, Warren—*Amicus Curiae*

Hutchins, John P.—Attorney, LeClairRyan

International Center for Law & Economics ("ICLE")—*Amicus Curiae*

Kilpatrick Townsend & Stockton LLP—Counsel for *Amicus Curiae* NFIB and former counsel for LabMD

LeClairRyan—Counsel for *Amici Curiae* ICLE and TechFreedom

Lehotsky, Steven P.—Attorney, U.S. Chamber Litigation Center

Manne, Geoffrey A.—Attorney, International Center for Law & Economics

Miliefsky, Gary—*Amicus Curiae*

Nabors, William L.—*Amicus Curiae*

National Federation of Independent Business Small Business Legal Center ("NFIB")—*Amicus Curiae*

National Technology Security Coalition ("NTSC")—*Amicus Curiae*

Norris, Cain M.—Attorney, Bois, Schiller & Flexner, LLP

Ohlhausen, Maureen K.—Acting Chairman and Commissioner, FTC (new title)

Park, John. J., Jr.—Attorney, Strickland Brockington Lewis, LLP.

Park, Michael H.—Attorney, Consovoy McCarthy Park PLLC

Ramirez, Edith—Commissioner and former Chairwoman, FTC (new title)

Ronald L. Raider—Attorney, Kilpatrick Townsend & Stockton LLP

Ross, Jr., Robert R.—*Amicus Curiae*

Singleton, Burleigh L.—Attorney, Kilpatrick Townsend & Stockton LLP

Stout, Kristian—Attorney, International Center for Law & Economics

Strickland Brockington Lewis, LLP—Counsel for *Amicus Curiae* Gary Miliefsky

TechFreedom—*Amicus Curiae* (before FTC and this Court)
(listed in LabMD's certificate solely as *Amicus Curiae* before agency)

Todd, Kate Comerford—Attorney, U.S. Chamber Litigation Center

U.S. Chamber Litigation Center—Counsel for *Amicus Curiae* Chamber of Commerce

STATEMENT REGARDING ORAL ARGUMENT

The Federal Trade Commission believes that oral argument may be helpful to the Court and therefore requests it.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

(Authorities principally relied upon are marked with an asterisk)

CASES

STATUTES

OTHER AUTHORITIES

REGULATIONS

STATEMENT OF THE ISSUES

1. Did the Federal Trade Commission properly find that LabMD's inadequate data security practices, which allowed sensitive private medical and financial data for 9,300 patients to be exposed to millions of internet users and downloaded at least once, were "unfair" under the Federal Trade Commission Act?

2. Did LabMD have fair notice that it had to take reasonable measures to protect consumers' personal data?

3. Does substantial evidence support the Commission's decision?

4. Is the Commission's remedial order within the scope of its discretion?

5. Can the Court remand for additional discovery, and if so, has LabMD shown any basis for a remand?

STATEMENT OF THE CASE

Every patient who obtains medical care—in practical terms, everyone in the country—undergoes medical tests at some point. The tests are conducted by laboratories that typically have no direct relationship with patients, but are privy to deeply personal information about them, including tests performed, their results, and diagnoses. If that information is revealed to a third party without permission, it violates the patient's right to privacy. Laboratories and other medical service providers also maintain other types of sensitive data, such as insurance information and Social Security numbers, that are appealing targets for data thieves.

Unauthorized disclosures of this data can lead to identity theft and other serious consequences. Yet patients are powerless to protect their personal information once it is in the testing laboratory's hands. They must rely on the company to keep it secure and confidential.

This case presents the question whether the Federal Trade Commission—the nation's premier consumer protection authority—can ensure the security and privacy of patients' sensitive medical information by holding businesses accountable when they harm consumers by failing to adequately safeguard that data. LabMD, a medical-testing laboratory, amassed a vast store of medical and other sensitive personal information for more than 750,000 patients on its computer system. But it systematically failed to use basic security measures to secure the data from unauthorized access. It did not adequately train its employees on data security dangers and prevention. It gave employees who did not need it access to sensitive patient information. It allowed employees to install risky, unapproved software on their computers. Its firewall was inadequate and improperly configured. And it had no intrusion detection system to warn it of unauthorized access to its network.

LabMD's culture of lax security culminated in a serious data breach. In 2005, an unauthorized file-sharing program was installed on a computer used by LabMD's billing manager. The program gave as many as 5 million internet users

at any given time direct access to files on her computer. For nearly a year beginning in 2007, one of the exposed files contained unencrypted medical and personal information for 9,300 patients. In effect, LabMD left that information out in plain view and allowed anyone to view its contents and download it. In 2008, LabMD learned that the file had been downloaded at least once.

The Commission held unanimously that LabMD's lax data security practices both harmed and were likely to harm consumers and thus were "unfair" under Section 5 of the FTC Act. It ordered LabMD to adopt reasonable security measures and to notify the 9,300 patients whose data it exposed. LabMD petitions for review.

A. Unfairness Under the FTC Act

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices" and directs the Commission to prevent them. 15 U.S.C. § 45(a)(1), (2). The statute gives the FTC broad discretion to "prevent such acts or practices which injuriously affect the general public." *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 967 (D.C. Cir. 1985) (quoting H.R. Rep. No. 1613, 75th Cong., 1st Sess. 3 (1937)). Congress "explicitly considered, and rejected, the notion" of "enumerating the particular practices to which [unfairness] was intended to apply." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-240 (1972); *see* H.R. Rep. No. 63-1142, at 19 (1914); S. Rep. No. 63-597, at 13 (1914). Instead, Congress "intentionally left

development of the term 'unfair' to the Commission" through case-by-case adjudication. *Atlantic Ref. Co. v. FTC*, 381 U.S. 357, 367 (1965); *see also Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1368 (11th Cir. 1988) (Congress gave the Commission a "broad mandate").

In 1980, the Commission issued a policy statement (the "*Unfairness Statement*") adopting standards to guide its exercise of unfairness authority.[1] It explained that "[u]njustified consumer injury is the primary focus of the FTC Act," and that to justify a finding of unfairness, the injury must satisfy three tests: it must be substantial; the costs of the injury must outweigh any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably avoid. 104 F.T.C. 949, 1073 (1984). The *Unfairness Statement* also explains that an injury "may be sufficiently substantial … if it raises a significant risk of concrete harm." *Id*. n.12. The Commission reaffirmed these principles in a 1982 letter to Congress, *see* H.R. Rep. No. 98-156, at 32-33 (1983) and in *International Harvester Co.*, 104 F.T.C. 949 (1984).

In 1994, Congress decided "to codify … the principles" of the *Unfairness Statement*. S. Rep. No. 103-130, at 12 (1993). It adopted the Commission's three-

[1] *Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction* (Dec. 17, 1980) (appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070-1076 (1984)).

prong test in new Section 5(n), which specifies that an act or practice may be deemed unfair only if it "[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

B. The FTC's Data Security Enforcement Program

The Commission has long used its unfairness authority to protect consumers from harms caused by the unauthorized exposure of their personal data. Computers and the internet promise immense benefits as they are integrated into every aspect of life and business, but the personal data held by companies poses corresponding risks of consumer harm, including privacy harms, identity theft, and fraud. Accordingly, the Commission has enforced Section 5 against dozens of companies, large and small, that failed to adequately protect consumers' personal information.[2] The Commission also provides extensive guidance to businesses on proper data security practices through written publications, videos, and other media.[3] The Third Circuit upheld the Commission's use of its unfairness authority to police data security in *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2014).

---

[2] *See* https://www.ftc.gov/enforcement/cases-proceedings/terms/249.

[3] *See* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

The Commission does not mandate data-security standards that companies must follow; technology and data-security threats continuously evolve, so what is appropriate today may not be tomorrow. Moreover, because companies vary widely in size and the type and volume of data they hold, a one-size-fits-all regime would be unworkable. Instead, the Commission has made clear that "[t]he touchstone of [its] approach to data security is reasonableness: 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." *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014).[4] The Commission "does not require perfect security," but only "reasonable and appropriate security"; it recognizes that "the mere fact that a breach occurred does not mean that a company has violated the law." *Id.*

Medical data is perhaps consumers' most sensitive information. Most people do not want their friends, colleagues, or even strangers to know what medications they take or diseases they may have. At a minimum, patients want to control whether and how that kind of information is released to others. Patients zealously guard not just diagnoses, but the fact of having taken diagnostic tests — many would not want to reveal that they have been tested for herpes, AIDS, or

[4] *See* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

cancer, for example. To ensure the privacy of such information the Commission has brought enforcement actions against companies that fail to reasonably protect medical data such as the email addresses of Prozac users, *Eli Lilly & Co.*, 133 F.T.C. 763, 767-768 (2002), and clinical notes from medical examinations, *GMR Transcription Servs.*, 2014 WL 4252393 (FTC Aug. 14. 2014).

In addition to medical data, testing laboratories like LabMD have access to other personal data, such as patients' insurance information and Social Security numbers. In the wrong hands, that information can cause significant harm. CX0741 at 5-6, 12-13; CX0742 at 13-16.[5] With a consumer's name and Social Security number, identity thieves can get direct access to bank and credit card accounts, make unauthorized purchases, or file fraudulent tax returns. CX0741 at 5; CX0742 at 10-11, 15. Armed with health insurance information, identity thieves can commit medical identity theft, fraudulently obtaining medical care (such as doctor's visits, procedures, or prescriptions) in the consumer's name. CX0741 at 13; CX0742 at 11, 13-16.

[5] Citations to "CX," "RX" and "JX" refer to trial exhibits. Page citations refer to the exhibit page number, rather than internal page numbers. "D" refers to document numbers in the list of administrative pleadings and filings in the Certified Index to the Record. "*Opinion*" and "*Order*" refer to the Commission's Final Opinion and Order, respectively (both at D355). "*MTD Order*" refers to the Commission's order denying LabMD's motion to dismiss (D48). "Tr." refers to the trial transcript. "Br." refers to LabMD's brief.

Identity theft can cause grave harm. Because consumers cannot easily change their names or Social Security numbers, unauthorized disclosure of such information "could result in affected consumers suffering fraud in perpetuity." CX0741 at 5, 12. Worse, stolen medical data can corrupt medical records with inaccurate information, potentially leading to misdiagnosis or unwarranted treatments. CX0742 at 15. Medical data theft has led to a black market in stolen information. CX0741 at 46, 51-52. One study showed that hackers can sell a health insurance credential on the black market for $20 and a complete medical record for $1200 or more.[6]

C. LabMD's Culture of Lax Data Security

LabMD provided medical testing services for physicians. LabMD collected confidential medical data on nearly all of its customers' patients so it would have data on any patient for whom a physician ordered a test. Tr. 1061-1066. All told, LabMD amassed data on more than 750,000 people. D326 at 20. LabMD collected and stored sensitive medical information, such as clinical histories, clinical testing information, medical record numbers, diagnosis codes and, where LabMD performed tests, the results of those tests. CX0443 at 4; JX0001 at 3. The

[6] *See* Dell SecureWorks, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents*, https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents.

patient profile also included other personal information such as names, addresses, birthdates, Social Security numbers, and insurance policy numbers. JX0001 at 3.

LabMD's compliance manual recognized the importance of keeping patient data "secure" and "private," and LabMD told its customers that this was part of the service it provided. CX0005 at 4; CX0704 at 128-129; CX0718 at 67-68. But in practice, LabMD failed to take basic precautions to safeguard the vast amount of sensitive patient data it held. LabMD's firewall was not designed to effectively assess risks or monitor network traffic to determine whether sensitive consumer information was being exported—a function easily attained with freely available software. CX0740 at 29. It did not regularly inspect computers, *e.g.*, for unauthorized or malicious software. *Id.* It had no intrusion detection or file integrity monitoring. *Id.* at 30. It did not perform penetration tests, available for as little as $450, to identify commonly known and easily fixed vulnerabilities. *Id.* at 30-31 & n.22. Compounding those problems, LabMD gave many employees administrative privileges that allowed them to install unauthorized software on their workstations. *Id.* at 37-38. It did not restrict access to sensitive data to those employees who needed it. *Id.* at 35-36. And as numerous employees testified, it made no effort to train employees on security risks or procedures for safeguarding sensitive patient information. *Id.* at 36-38; *see Opinion* 14 nn.40-42.

LabMD's lax security practices ultimately resulted in a public release of 9,300 consumers' confidential data. In 2005, a peer-to-peer file-sharing program called LimeWire was installed on a computer used by LabMD's billing manager. CX0755 at 4. Peer-to-peer programs allow computer users to easily locate and share files over the internet. Although these programs are commonly used to share music and videos, users can browse shared directories and download any file another user has designated for sharing. Tr. 844-845; CX0738 ¶¶14, 22, 29; RX533 at 16. LimeWire connected to the "Gnutella" network, which had 2 to 5 million people logged-in at any given time. Tr. 833, 1181; CX0738 ¶60; RX0533 at 15. Peer-to-peer networks like Gnutella are a known target for identity thieves, who see them as easy pickings for personal data. Tr. 868; CX0738 ¶65; Tr. 1376-1377, 1380-1381.

The contents of the "My Documents" folder on the billing manager's computer were designated for sharing. CX0730 at 3, 7-8. Anyone connected to the Gnutella network thus had free access to anything in that folder or its subfolders. Because LabMD later destroyed the computer's hard drive (CX0710 at 51-52) it is not possible to know how many unauthorized persons saw sensitive data from the billing manager's computer. What is known, however, is that from June 2007 to May 2008 the computer's "My Documents" folder contained a 1,718-page file (the "1718 file") with personal information of 9,300 consumers, including

their names; dates of birth; Social Security numbers; laboratory test codes; and, for some, health insurance company names, addresses, and policy numbers. CX0766 at 8; D9 ¶19. It also contained three other files with similar sensitive information. Tr. 1404-1406; RX0645 at 39, 42-43. During that 11-month period, any of the millions of Gnutella users could have discovered and downloaded these files. Tr. 1371-1372; CX0738 ¶¶56-76.

At least one user, the data security company Tiversa, did download the files. It shared the 1718 file with an academic researcher and attempted to use the security breach to solicit LabMD as a customer. Tr. 1371-1372; CX0766 at 8-9. LabMD responded by removing LimeWire from the billing manager's computer in 2008, but never notified any of the 9,300 affected patients that their personal information had been compromised. Tr. 1087.

LabMD improperly describes the download as "theft." Br. 7. But it was LabMD's lax security that allowed the file to be made public. Courts uniformly hold that peer-to-peer network users are not thieves, but the intended recipients of files shared over those networks. *E.g.*, *United States v. Pirosko* 787 F.3d 358 (6th Cir. 2015). As one court put it, "One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking." *United States v. Stults*, 575 F.3d 834, 842-843 (8th Cir. 2009).

The security breach and LabMD's failure to detect it are directly traceable to the company's lax security culture. Had LabMD limited employees' administrative privileges, LimeWire would not have been installed on the billing manager's computer. Tr. 199, 201-202. Had it provided adequate security training, its employees would likely have understood the risks of installing file-sharing software. *See* CX0740 at 37-38. And had LabMD adequately monitored its system—or even made routine walk-around inspections of employee computers—it would likely have detected the threat posed by the unauthorized LimeWire installation. *See* CX0740 at 25; CX0707 at 24.

D. Administrative Proceedings

After a lengthy investigation, the Commission in 2013 initiated an administrative proceeding to determine whether LabMD's data security practices were unfair under Section 5. LabMD almost immediately decided to cease its testing operations (though it continued to store data for 750,000 patients on its computer system).[7] Following a trial, the administrative law judge dismissed the

[7] LabMD claims that the FTC "destroyed" its business. *E.g.*, Br. 1. There is no evidence to support this assertion. LabMD was highly profitable, with a profit margin of 25 percent on annual revenue that reached $10 million, and it was represented before the FTC by pro bono counsel. Tr. 978, 1058-1059; CX0709 at 32.

complaint on the ground that FTC trial counsel had not proved that LabMD's data security practices caused or were likely to cause substantial consumer injury.[8]

The Commission reversed. It found that LabMD's data security measures were inadequate in multiple respects. Those failings led to installation of LimeWire, which in turn led to sharing the 1718 file on LimeWire and Tiversa's download. Sharing the file both caused and was likely to cause substantial and unjustified consumer injury.[9]

First, the Commission found that disclosure of the 1718 file to Tiversa caused actual harm. It held that release of a patient's medical information by itself is "substantial injury," even if unaccompanied by proof of economic harm or bodily injury. *Opinion* 17-19. The Commission explained that while most cases of unfairness involve economic injuries or health and safety harms, neither the *Unfairness Statement* nor Section 5(n) foreclosed a finding that "an intangible but very real harm like a privacy harm" may be a "substantial injury." *Opinion* 10. The Commission noted that patient privacy interests in their medical data have long been recognized by Congress, States, and the common law. *Opinion* 18-19.

[8] At trial, it was revealed that Tiversa's CEO falsely testified that the 1718 file had spread to other internet locations. Trial counsel disclaimed reliance on this testimony and neither the ALJ nor the Commission gave it any weight.

[9] The Commission focused principally on the 1718 file, but noted that the three other files containing sensitive personal information downloaded by Tiversa raised similar concerns. *Opinion* 3 n.11.

Independently, the Commission found that the exposure of the 1718 file on the Gnutella peer-to-peer network to millions of potential viewers for eleven months was "likely to cause substantial injury." *Opinion* 20. It found "a high likelihood of harm" because the file could have been found by any Gnutella user, some of whom were malicious users searching for confidential information. *Opinion* 21-23. The Commission also found that "the severity and magnitude of potential harm was high." *Opinion* 21-24. It focused on the risk of both ordinary and medical identity theft, which could cause the affected consumers monetary losses and endanger their health and safety. *Opinion* 24-25. It also reiterated that unauthorized release of sensitive medical data is a privacy harm in itself. *Id*.

The Commission found the second and third prongs of Section 5(n) satisfied. Consumers could not reasonably avoid injury from LabMD's data-security failures and there were no countervailing benefits to its faulty security. *Opinion* 25-28. LabMD could easily have prevented the harm using free or inexpensive software tools and low-cost, commonsense practices, such as training employees and restricting privileges to prevent them from installing unapproved software. *Opinion* 26-28.

To prevent recurrence of consumer harm and protect the 750,000 consumers whose data LabMD still has, the Commission ordered LabMD to adopt a "reasonably designed" program appropriate to the nature and scope of its current

activities. *Order* 2. LabMD must biannually obtain an independent assessment of the program and must also notify the 9,300 individuals whose personal information was exposed. *Order* 3-4. This Court stayed those remedial provisions.

E. Standard of Review

The Court reviews the Commission's legal conclusions *de novo*, but must give "some deference to the Commission's informed judgment that a particular commercial practice is to be condemned as 'unfair.'" *FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447, 454 (1986); *see also Atlantic Ref.*, 381 U.S. at 368 ("[W]e give great weight to the Commission's conclusion.") (internal quotation marks omitted).

The Commission's interpretation of Section 5(n) is reviewed under *Chevron USA Inc. v. NRDC*, 467 U.S. 837 (1984). If "Congress has not directly addressed the precise question at issue," the Court must defer to the Commission's interpretation as long as it "is based on a permissible construction of the statute." *Id*. at 842-843.

This Court reviews the Commission's findings of facts under the "substantial evidence" standard." *McWane, Inc. v. FTC*, 783 F.3d 814, 824 (11th Cir. 2015). Substantial evidence means "more than a mere scintilla" of evidence, "but less than a preponderance." *Dyer v. Barnhart*, 395 F.3d 1206, 1210 (11th Cir. 2005). Evidence is sufficient if "a reasonable mind might accept [it] as adequate to

support a conclusion." *Schering-Plough Corp. v. FTC*, 402 F.3d 1056, 1062 (11th Cir. 2005). The Court may not "make its own appraisal of the testimony, picking and choosing for itself among uncertain and conflicting inferences." *McWane*, 783 F.3d at 824 (internal quotation marks omitted). The standard of review remains the same "regardless [of] whether the FTC agrees with the ALJ." *Schering-Plough*, 402 F.3d at 1062.

SUMMARY OF ARGUMENT

LabMD collected deeply private health data about 750,000 patients who could not protect their information once it was in LabMD's hands. The company knew it needed to keep the data secure and confidential—it promised its clients that it would do so and told its employees that disclosure was illegal—but nevertheless failed to take some of the most basic steps toward reasonable security. LabMD failed to train its staff about data security. It gave employees access to sensitive patient information they did not need for their jobs. It failed to prevent the installation of risky software. It failed to use widely available and inexpensive tools to monitor its network and identify security vulnerabilities. The upshot was as inevitable as it was predictable: the public exposure of private patient data to millions of potential viewers across the internet.

The Commission found LabMD's lax security practices unfair to patients in violation of the FTC Act in two ways. First, the disclosure of the 1718 file to

Tiversa caused a direct substantial injury: an invasion of patient privacy. Second, leaving the file open for viewing by millions of internet users for nearly a year was likely to cause substantial injury. Unrepentant and still unconcerned with the welfare of the people whose medical data it leaked, LabMD now claims that its behavior is beyond the FTC's reach. Its arguments are meritless.

1.a. The Commission properly ruled that the broad statutory term "substantial injury" includes the intangible but concrete ham caused by the disclosure of sensitive medical information. The law has long recognized that public disclosure of private information is by itself an actual concrete harm, even absent tangible effects or emotional injury. The harm occurs even when the victim of the disclosure, like LabMD's victims, are unaware that their private information has been disclosed.

LabMD is wrong that the plain language of Section 5(n) excludes intangible injury. The statute does not use the word "tangible," and the Court should not read it into the text. Nor does the Senate Report or the Commission's *Unfairness Statement* supply a plain meaning that the statute itself does not contain. In the *Unfairness Statement*, the Commission stated that cases of pure "emotional impact" without tangible injury "ordinarily" do not amount to substantial injury. But that does not suggest that the Commission or Congress intended to exclude other intangible but concrete injury—like invasion of privacy—from the statute's

broad scope. Indeed, shortly after the Commission issued the *Unfairness Statement*, it brought a case based in part on an intangible injury. The statute gives the Commission broad authority, and its interpretation is reasonable under *Chevron*. The Commission's reading is bolstered by the strong public policies that protect privacy, established in its past decisions, federal statutes and case law recognizing the harm caused by disclosure of sensitive medical information.

b. The Commission properly determined that the exposure of the 1718 file to millions of internet users for 11 months was "likely to cause substantial injury." The Commission found a "high" likelihood of injury, which satisfies any reasonable definition of "likely." The Court can uphold the decision on that ground alone. But the Commission did not err in any case in holding that the phrase "likely to cause substantial injury," read as a whole, incorporates both the probability and the magnitude of harm, so that a lower probability will suffice if the magnitude of the harm is sufficiently great. The Commission had explicitly held as much twice before Congress enacted Section 5(n). LabMD is not rendered immune because its unlawful conduct took place in the past. The plain language of Section 5 makes clear that it applies where a company "*has been* or is" violating the statute.

c. The Commission properly conducted the Section 5(n) cost-benefit analysis, finding that LabMD's multiple security failures could have been fixed

inexpensively and conferred no benefit on consumers. Contrary to LabMD's unsupported assertion, legislative history and past Commission decisions make clear that the Commission need not precisely quantify risks and benefits. That is especially so here, where the harms are clear and there is no conceivable benefit.

d. LabMD's argument that the Commission can show unfairness only if it proves factors—such as egregiousness, deception, or recklessness—beyond those specified in Section 5(n) is contrary to the plain language of the statute and was rejected by this Court in *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354 (11th Cir. 1988).

e. The Commission properly considered all of LabMD's multiple security failings in reaching its determination that LabMD acted unfairly. The sharing of the 1718 file was the specific cause of injury to LabMD's patients, but that harm was merely the end result of LabMD's long-running failure to ensure the security of the patient information it held.

f. The Health Insurance Portability and Accountability Act ("HIPAA") does not implicitly repeal Section 5(n) as applied to medical information. LabMD identifies nothing to suggest that Congress intended to repeal the FTC's authority. Nor does it identify any inconsistency in the two statutes. The FTC Act does not require any behavior HIPAA forbids, nor does HIPAA require any conduct the FTC Act forbids. No conflict means no implied repeal.

2. The Commission's unfairness finding did not violate due process. LabMD had ample notice of the need to take reasonable steps protect patient data, which is all the statute requires or the Commission expects. Indeed, the company promised its physician customers that it would keep data secure and it warned its employees that the law required them to protect patient privacy. As the Third Circuit recently held in *Wyndham*, Section 5(n) itself provides constitutionally adequate fair notice to businesses that they may be subject to FTC Act liability for data security practices that cause substantial and unjustified consumer injury. This Court has held similarly that commercial statutes like the FTC Act satisfy fair notice principles unless they are effectively incomprehensible.

Principles of due process do not require that LabMD had "ascertainable certainty" as to the specific security measures it needed to take. That standard applies only where an agency seeks to impose a monetary penalty, which the Commission did not and could not do here. Nor does due process demand that the FTC promulgate data security rules. It is long settled that agency may develop and apply standards through case-by-case adjudication, rather than up-front rulemaking. In any case, LabMD had substantial guidance as to what kinds of security measures were reasonable through written guidance documents from the FTC and other agencies and prior Commission complaints and consent decrees in data security cases.

3. Substantial evidence supports the Commission's decision. The Commission considered all the evidence—including the evidence that LabMD says it ignored—and drew reasonable inferences from it. Nothing in the record compels a conclusion different from the Commission's, and LabMD has shown no basis to second-guess the Commission's fact finding.

4. The Commission properly exercised its broad discretion in selecting a remedy for LabMD's data security failures. LabMD's removal of LimeWire from its system did not cure the wholesale security failures identified by the Commission, nor did it deprive the Commission of further authority. Similarly, LabMD's decision to cease active operations for now does not strip the Commission of power. The company's owner testified that he would try to resume the business once this case is over, and LabMD continues to hold sensitive data for 750,000 patients. Consumers must be protected by reasonable data security measures in the meantime. The Commission also had authority to require notice to the 9,300 patients whose personal data was exposed. Notice in this circumstance is directly akin to corrective advertising, a remedy long approved by the courts. LabMD has waived its vagueness challenge to the Commission's order, but in any case the Commission's detailed order is not vague.

5. LabMD cannot avail itself of Section 5(c)'s authorization of a remand to "adduce additional evidence." It seeks only to take additional discovery, a

remedy not covered by the statute. Even if the statute allowed remand, LabMD has not satisfied the statutory prerequisites. The discovery sought—evidence that the FTC violated the Fourth Amendment in obtaining the 1718 file—cannot be material because LabMD had no expectation of privacy for materials placed on a peer-to-peer network. And LabMD has already taken a deposition from the FTC on how it came to possess the 1718 file.

LabMD waived its claim of retaliation, but it is frivolous in any event. The filing of a complaint shortly after publication of a critical book is plainly meaningless in the context of an investigation that had been pending for three years. LabMD points to nothing that remotely suggests that the FTC Commissioners did not discharge their official duties in good faith.

ARGUMENT

I. THE COMMISSION PROPERLY APPLIED SECTION 5(n) IN FINDING THAT LABMD'S LAX DATA SECURITY PRACTICES WERE UNFAIR.

LabMD argues that the Commission committed a series of legal errors in finding that its lax data security practices were unfair under Section 5.[10] The Commission applied Section 5(n) and held that disclosure of the 1718 file to Tiversa caused actual harm—an invasion-of-privacy injury—and that the public

[10] The Third Circuit has upheld the FTC's authority to police data security. *Wyndham*, 799 F.3d at 244-249. Some *amici* seek to relitigate this issue, but LabMD does not, and this Court does not consider arguments not raised by the appellant. *E.g.*, *Richardson v. Ala. St. Bd. of Educ.*, 935 F.2d 1240, 1247 (11th Cir. 1991).

availability of the file was also likely to cause harm given the millions of users with unfettered access to the file over eleven months. Either ground is sufficient to uphold the Commission's decision. The Commission also concluded that the harm was not reasonably avoidable by consumers and was not outweighed by countervailing benefits. LabMD's multiple challenges are meritless.

A. The Commission Reasonably Concluded That Unauthorized Disclosure of Medical Data Is a Substantial Injury.

The Commission determined that "the disclosure of sensitive health or medical information causes … harms that are neither economic nor physical in nature but are nonetheless real and substantial" within the meaning of Section 5(n). *Opinion* 17. That holding was consistent with longstanding principles enshrined in the common law, federal statutes, and past Commission decisions. LabMD contends that the "plain meaning" of "substantial injury" encompasses only tangible injuries. Br. 14. But neither the statute nor its legislative history indicates that privacy harm cannot be "substantial injury." The Commission's reading of the statute was reasonable and is entitled to *Chevron* deference.

1. Disclosure of sensitive medical information is by itself a concrete privacy harm.

The gist of LabMD's argument is that invasion of medical privacy is merely an "emotional" harm that Congress excluded from the coverage of Section 5(n). While there is no question that unauthorized disclosure of sensitive medical

information can cause severe emotional harm, the Commission found that under established principles of privacy law and consistent Commission practice, invasion of medical privacy is also by itself an actual concrete harm that fits firmly within the statute's coverage. *See Unfairness Statement*, 104 F.T.C. at 1073 n.12 (an injury is unfair "if it raises a significant risk of concrete harm").

The Commission has long viewed medical information as highly sensitive and has taken actions to prevent businesses from disclosing such information without patient consent.[11] Courts likewise treat medical data as "the most sensitive kind of information." *Maracich v. Spears*, 133 S.Ct. 2191, 2202 (2013). This Court has recognized, for example, the "significant" and "constitutionally-protected" interest in preventing non-consensual disclosure of HIV-positive diagnoses. *Harris v. Thigpen*, 941 F.2d 1495, 1513-1514 (11th Cir. 1991). Similarly, the common-law invasion-of-privacy tort protects sensitive personal information—including medical information—from unauthorized disclosure. *See Restatement (Second) of Torts* § 652D (1977) ("*Restatement*"). Courts applying

[11] The Commission's very first data security case, in 2002, addressed lax data security procedures that caused disclosure of the email addresses of Prozac users. *See Eli Lilly*, 133 F.T.C. at 767-768. More recently, the Commission has brought cases against a company that disclosed notes of medical examinations on the internet, *GMR Transcription Servs.*, 2014 WL 4252393, and a company that solicited consumer healthcare reviews without indicating that the reviews would be publicly posted on the internet, *Practice Fusion, Inc.*, 2016 WL 3345406 (FTC June 8, 2016).

that principle have long found that the unauthorized disclosure of patients' medical information is actionable invasion of privacy. *E.g.*, *Horne v. Patton*, 287 So.2d 824, 830-831 (Ala. 1973).[12]

Tort law recognizes that an invasion of privacy is itself a concrete harm even without any tangible or economic loss or emotional harm. The *Restatement* explains that a plaintiff may recover for "the harm to his interest in privacy resulting from the invasion," separate and apart from any "mental distress" or "special" (*i.e.*, monetary) harms. *Restatement* § 652H. Indeed, because invasion of privacy is an independent harm, plaintiffs can recover presumed damages for that injury "without reference to specific harm." *Doe v. Chao*, 540 U.S. 614, 621 (2004).

Applying these principles, the Third Circuit recently recognized that disclosure of sensitive medical information is an actual concrete harm sufficient to confer standing even absent any tangible harm. *In re Horizon Healthcare Servs. Inc. Data Security Breach Litig.*, 2017 WL 242554 (3d Cir. Jan. 20, 2017). There, a health insurer stored unencrypted medical information on laptop computers, which were stolen. Although plaintiffs did not argue that the stolen information

[12] Thus, state courts have held that the disclosure of an AIDS diagnosis is an invasion of privacy, *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E.2d 491 (Ga. App. 1994), and that disclosure of confidential medical records would cause irreparable harm, *S.P. v. Vecchio*, 162 So. 3d 75, 79 (Fla. App. 2014).

was used to their detriment, they nonetheless argued that they had suffered a "concrete" privacy injury. The Third Circuit agreed, holding that "unauthorized disclosures of information have long been seen as injurious" and that "improper dissemination of information can itself constitute a cognizable injury." *Id.* at *10 (citation and internal quotation marks omitted); *see also id.* at *13 (Shwartz, J., concurring) ("the intangible harm from the loss of privacy" satisfies the "concrete harm" requirement for standing).

2. Neither the text nor the legislative history of Section 5(n) prohibits liability for intangible injury like privacy harms from the release of medical data.

Despite the established legal understanding of privacy harm as a concrete injury, LabMD argues (Br. 13-16) that the "plain meaning" of "substantial injury" in Section 5(n) is limited to "tangible injury" and excludes intangible privacy harms. But Section 5(n) does not use the word "tangible"; LabMD simply asks the Court to read that term into the text. The plain language of Section 5(n) thus does not address "the precise question" whether "substantial injury" can include the concrete but intangible injury from disclosure of one's sensitive medical information. *Chevron*, 467 U.S. at 842. LabMD does not seriously contend otherwise.

The *Unfairness Statement* and the Senate Report do not show any legislative intent to exclude from the broad language of the statute the concrete but intangible

harm caused by invasion of privacy. The Senate Report does not use the term "intangible" in discussing Section 5(n). The *Unfairness Statement* states directly that "[a]n injury can be sufficiently substantial if it … raises a significant risk of *concrete* harm." 104 F.T.C. at 1073 n.12 (emphasis added). The Supreme Court recognized just last year that even intangible injuries can be concrete. The Court explained that "[a]lthough tangible injuries are perhaps easier to recognize, … intangible injuries can nevertheless be concrete." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016). This is especially true where, as here, the intangible harm "has a close relationship to a harm"—such as invasion of privacy—"that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.*

Nor does it help LabMD that the *Unfairness Statement* states that "emotional impact" and other "more subjective" types of harms "ordinarily" do not amount to substantial injury unless a tangible injury can also be demonstrated. *Unfairness Statement*, 104 F.T.C. at 1073 & n.16; *see* S. Rep. No. 103-130 at 13 ("Emotional impact and more subjective types of harm alone are not intended to make an injury unfair."). Nothing in the discussion of "emotional" harms in the *Unfairness Statement* or the Senate Report remotely suggests that the Commission or Congress intended to exclude *all* intangible harms. Indeed, just a few years after issuing the *Unfairness Statement*, the Commission brought an unfairness case

for breach of a service contract based in part on the "intangible loss of the certainty of the fixed price term in the contract." *Orkin Exterminating Co.*, 108 F.T.C. 263, 362 (1986). This Court affirmed. *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354 (11th Cir. 1988). These decisions were part of Congress's background understanding of unfairness when it enacted Section 5(n).

Under the law, an invasion-of-privacy harm is not purely emotional or subjective. As shown above, invasion of privacy has long been recognized as a concrete harm separate and distinct from "mental distress." *Restatement* § 652H. Indeed, LabMD's victims (like many victims of data breach) have experienced no emotional harm because they are not even aware that their personal information has been exposed (LabMD has never told them). Yet, as the law recognizes, they still have been concretely harmed, because sensitive information that they expected would be kept private has been exposed and accessed by unauthorized persons. Such a harm does not depend on the victim's mental state. It bears no resemblance to an offense to taste or social beliefs, the examples of emotional harm in the *Unfairness Statement*. 104 F.T.C. at 1073. It is more akin to trespass, another common-law tort, which makes the trespasser liable whether or not the property owner suffers tangible injury. *See Restatement* § 163.

3. Established public policies further support the Commission's reading of "substantial injury" to include privacy harms from unauthorized release of medical data.

As explained above, the Commission's reading of "substantial injury" was reasonable given consumer expectations that their sensitive medical data will be kept secure and its solid grounding in common law, judicial decisions, and Commission practice. That interpretation is supported further by Congress's direction in Section 5(n) that "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." 15 U.S.C. § 45(n). In addition to the statutory language, legislative history, and legal understanding of privacy harms, the Commission also considered a range of public policies that support its conclusion that disclosure of sensitive medical information is "substantial injury."

As shown above, the common law has long recognized violation of privacy as a distinct harm that causes cognizable and remediable injury. Congress has incorporated the common-law understanding of privacy harm as a significant, concrete injury through numerous statutes that protect medical privacy rights. In HIPAA, it directed the Department of Health and Human Services to issue rules protecting medical data. Pub. L. No. 104-191 § 264, 110 Stat. 1936 (1996); Privacy and Security Rules, 45 C.F.R. Parts 160, 164. The Fair Credit Reporting Act prohibits the release of "medical information … about a consumer." *Id*.

§ 1681b(g)(1). The Privacy Act likewise protects medical information, 5 U.S.C. § 552a(a)(4), (b), as does the Freedom of Information Act, which exempts from public disclosure "medical files … the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). Furthermore federal and state courts have also recognized the importance of protecting the confidentiality of sensitive medical information. *Opinion* 19; *see also* cases cited *supra* at 24-25 & n.25.

The longstanding policy recognition that unauthorized disclosure of sensitive medical information is a concrete injury that deserves legal protection bolsters the Commission's reading of the statutory term "substantial injury" to include privacy harms from the disclosure of such information. Because that reading is a permissible construction of the statute and there is no dispute that LabMD actually disclosed sensitive medical information to Tiversa, the Commission properly held that LabMD's lax data security caused "substantial injury" in the form of an actual and concrete privacy harm.

B. The Commission Reasonably Concluded That Exposure of the 1718 File Was Likely To Cause Substantial Injury.

The FTC Act does not require the Commission to wait until harm actually occurs before taking action. Congress directed the Commission to "prevent" unfair practices and permitted the Commission to find a practice unfair if it is "likely to cause substantial injury." 15 U.S.C § 45(a)(2), (n). Here, in addition to finding an

actual privacy harm, the Commission held as an independent ground for its decision that public exposure of the 1718 file to millions of internet users for 11 months was "likely to cause substantial injury" to patients, including identity theft. LabMD argues that the Commission improperly defined "likely." Alternatively, it argues that a finding of likely harm cannot be based on conduct that has ceased. Both claims fail.

1. The Commission properly held that harm was "likely" to occur.

LabMD's argument that the Commission misconstrued "likely" is based entirely on the Commission's statement that "a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low." *Opinion* 21. Focusing solely on this isolated statement, LabMD (and several *amici*) argue that the Commission "reduced beyond recognition" the meaning of "likely." Br. 19.

LabMD's argument is a smokescreen. *This* case does not involve a low probability of harm. The Commission found that the exposure of the 1718 file to millions of internet users over eleven months created a "*high* likelihood of harm." *Opinion* 21 (emphasis added). It also found that "the severity and magnitude of potential harm was high," including the risk of both medical and ordinary identity theft. *Opinion* 24-25. LabMD does not challenge the Commission's finding that release of this information could substantially harm patients. Whether a lower

probability would also have satisfied the unfairness standard given the severity and magnitude of potential harm is not at issue.

As the Commission explained, the likelihood of harm was high because 1718 file was exposed to millions of users who easily could have found it—the equivalent of leaving your wallet on a crowded sidewalk. It cited evidence that with 2 to 5 million LimeWire users online at any given time, "[o]ver an extended period of time, such as weeks or months, even a 1 in 1,000,000 chance of someone downloading the 1,718 file would result in it being downloaded many times." *Opinion* 23. The Commission also noted that "malicious users" deliberately search peer-to-peer networks to obtain information they can use or sell. *Opinion* 22. Since Tiversa easily found the 1718 file, data thieves who target such information could have done so as well. Notably, in 2012 police found LabMD documents containing the personal information of 600 patients (including names and Social Security numbers) in the hands of identity thieves in California. *Opinion* 4. Although the Commission did not find that this incident warranted an independent unfairness finding, it illustrates that data thieves sought from LabMD precisely the type of information contained in the 1718 file.

Given the millions of people to whom the data was exposed for nearly a year, the Commission's finding of a "high" likelihood of harm satisfies

Section 5(n)'s "likely" requirement under any reasonable definition of that word—including the definition proposed by LabMD.[13]

Even if the precise scope of "likely to cause substantial injury" were at issue here, the Commission's reading is consistent with ordinary rules of statutory construction and its own prior decisions. The Commission explained that it reads the phrase as requiring a risk assessment that turns on both "the likelihood or probability of the injury occurring and the magnitude or seriousness of the injury if it does occur." *Opinion* 10. That is consistent with the way the Third Circuit read the statute in *Wyndham*, where the court explained that the Section 5(n) cost-benefit analysis "considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers." 799 F.3d at 255.

LabMD is wrong that the likelihood and magnitude of harm must be considered piecemeal as separate and unrelated requirements. As this Court recently held, "[w]ords can acquire different meanings when combined in a phrase," and a phrase is thus "different from the sum of its parts." *Villarreal v.*

[13] LabMD cherry-picks definitions, relying exclusively on a single online dictionary. Like many common words, "likely" has a range of meanings. For example, another leading dictionary defines "likely" as "[w]ithin the realm of credibility; plausible." *American Heritage Dictionary* 1042 (3d ed. 1992). The Commission concluded that dictionaries were not a useful guide for this purpose and looked instead to the *Unfairness Statement* and past Commission practice for guidance. *Opinion* 20-21.

R.J. Reynolds Tobacco Co., 839 F.3d 958, 964 (11th Cir. 2016) (en banc). The plain language of the phrase "likely to cause substantial injury" indicates that it refers jointly to both the probability of an injury and its magnitude. As the Commission explained, the most natural reading of the entire phrase thus indicates that it is meant to incorporate the overall risk of a serious consumer harm from a given practice. *See Opinion* 21.[14]

That reading is supported by prior Commission decisions that were well known when Congress codified the *Unfairness Statement* in Section 5(n). In *International Harvester*, the Commission found a failure to warn consumers of a life-threatening product defect to be unfair even though accidents had occurred at a rate of only 0.001% over 40 years. *International Harvester*, 104 F.T.C. at 1063.[15] Though the chance of an incident was low, combined with the magnitude of potential harm, the practice posed a high risk of injury overall. In *Philip Morris*,

[14] The Commission's construction is similar to the way some courts evaluate the "likely to succeed on the merits" standard in the context of preliminary relief, using a sliding scale that balances the chance of success against the magnitude of harm. *See, e.g.*, *Revel AC, Inc. v. IDEA Boardwalk LLC*, 802 F.3d 558, 567-571 (3d Cir. 2015). In that approach, "likely to succeed" means having a chance of success that is "better than negligible," but need not be "more likely than not." *Id.* at 569.

[15] LabMD tries to distinguish *International Harvester* on the ground that harm had already occurred in that case, but the Commission made clear that "unfairness cases may also be brought on the basis of likely rather than actual injury." 104 F.T.C. at 1061 n.45. The Commission could have taken the same action before the first injury occurred.

82 F.T.C. 16 (1973), the Commission found that unsolicited distribution of razor blades in newspapers was unfair because of the potential safety risk to children, even though no injuries had occurred.[16] Like *International Harvester*, the risk of injury to a given child was low, but the potential harm was great.

In light of this history, the Commission reasonably and properly read the phrase "likely to cause substantial injury" as a coherent unit, in which the likelihood of harm is assessed in relation to the magnitude of injury.

2. LabMD's past conduct supports an unfairness finding.

LabMD next claims that the Commission could not find unfairness based on the likelihood of injury from past conduct that has now ceased. Br. 22-23. It argues that the statute uses the term "is likely" in the present tense, whereas in analyzing LabMD's conduct the Commission assessed only whether harm "was likely," in the past tense.

The argument fails on the plain language of Section 5, which expressly authorizes the Commission to take enforcement action whenever it finds that a company "*has been* or is using" an unfair method or practice. 15 U.S.C. § 45(b) (emphasis added). Congress thus plainly intended that the Commission would have authority to take action against businesses that have engaged in harmful

[16] LabMD argues that *Philip Morris* merits no weight because it was a consent decree. But the matter was cited in the *Unfairness Statement*—the basis for Section 5(n)—as an example of the type of conduct that could be deemed likely to cause unjustified consumer injury. 104 F.T.C. at 1073 n.15.

conduct, even if that conduct is no longer ongoing. LabMD's reading would improperly strike the phrase "has been … using" from the statute, contrary to the well-settled rule that courts must "give effect to all statutory provisions and construe related provisions in harmony with each other." *United States v. Drury*, 344 F.3d 1089, 1098 (11th Cir. 2003). It also would allow malfeasors to evade FTC enforcement by stopping their illegal behavior upon learning of an FTC investigation.

Ordinary rules of English usage reinforce reading Section 5(n) in harmony with Section 5(b). As this Court's predecessor explained, "the present tense of a verb may sometimes refer to the past and to the future as well as to the present" and "may be used when the time is actually indefinite." *In re Stratford of Texas, Inc.*, 635 F.2d 365, 369 (5th Cir. 1981) (citing R. Pence and D. Emery, *A Grammar of Present-Day English* 262-263 (2d ed.)). The simple present tense may also be used where the action is "habitual or timeless." Bernard T. O'Dwyer, *Modern English Structures: Form Function and Position* 116 (2d ed. 2006). The phrase "causes or is likely to cause" uses this form of the present tense; it cannot plausibly be read to encompass only conduct that continues until the date of the Commission's order. And even if it could, that would merely create an ambiguity, given Section 5(b)'s express reference to past conduct. *See Stratford*, 635 F.2d at

369 (the present tense is "not without some ambiguity"). To the extent there is an ambiguity, the Commission's reading is reasonable.

C. The Commission Properly Balanced Benefits and Costs.

Section 5(n) requires the Commission to conduct a cost-benefit analysis to determine whether the potential harm to consumers from a practice is "outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). LabMD argues that the Commission failed to fulfill that requirement. Br. 23-26, 32-35. In fact, the Commission conducted the analysis and concluded that LabMD's security practices "easily satisfied" the test. *Opinion* 26-28.

The Commission's task was to weigh the harm to consumers against any "countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). The harms caused by inadequate data security practices are clear. *See* pp.6-8, *supra.* On the other side of the equation, the Commission explained that "[a] 'benefit' can be in the form of lower costs and then potentially lower prices for consumers." *Opinion* 26. The Commission found no such benefit because LabMD's data security failures could have been remedied with inexpensive solutions: free or low-cost tools for detecting vulnerabilities, training in data security for its employees, steps to limit access to personal information on LabMD's system, and providing employees with non-administrative accounts so that they could not install unauthorized software. *Opinion* 27-28. Because the cost of implementing these

measures would have been low, any benefits to consumers from lax security were "negligible." *Id.*

LabMD pulls from thin air a complex mathematical cost-benefit formula that it says that the Commission was required to apply. Br. 24. The formula is unmoored from anything in the statute. Section 5(n) requires the Commission to assess whether the harm to consumers from a practice is outweighed by countervailing benefits to them. That is precisely what the Commission did—and it found no significant countervailing benefits.

Nor does Section 5(n) require the Commission to precisely quantify the magnitude of consumer injury or the costs of averting that injury. Br. 24-26. The 1993 Senate Report makes clear to the contrary that Congress did "not intend that the FTC quantify the detrimental and beneficial effects of the practice in every case. In many instances, such a numerical benefit-cost analysis would be unnecessary; in other cases, it may be impossible." S. Rep. No. 103-130, at 13. That approach is consistent with the Commission's explanation in *International Harvester* that "we do not strive for an unrealistic degree of precision, valuing an injury or a life at precisely *x* many dollars. We assess the matter in a more general way, giving consumers the benefit of the doubt in close issues." 104 F.T.C. at 1065 n.59. This case is not a close one; the potential harm is substantial and there

are no significant countervailing benefits that outweigh the harm to consumers. No further analysis was necessary.

Finally, LabMD argues that the Commission was required to conduct yet another cost-benefit analysis to support its conclusion that LabMD's lax data security was unreasonable. Br. 32-35. But "unreasonable" is simply a shorthand way of saying that the Section 5(n) unfairness analysis is satisfied. Data security practices are unreasonable—*i.e.*, unfair—if they cause a substantial, unavoidable injury to consumers with no corresponding benefit. Thus no additional cost benefit analysis is required beyond that set forth in Section 5(n) and the *Unfairness Statement*.

D. There Are No Additional Requirements for Unfairness Beyond the Section 5(n) Factors.

LabMD argues that even if the Section 5(n) test is satisfied, a practice may not be deemed unfair unless it is also "deceptive," "reckless," or "egregious." Br. 26-28. In *Orkin*, this Court rejected a virtually identical request to graft extra words onto the definition of unfairness.[17] Orkin argued that a "mere breach of

[17] LabMD ignores *Orkin* and instead cites dictum in *LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185 (11th Cir. 2010), that one dictionary defines unfair is "marked by injustice, partiality or deception." *Id.* at 1200. But as the Third Circuit explained in *Wyndham*, citing the same definition, "[w]hether these are requirements of an unfairness claim makes little difference"; an unjustified consumer injury meets the standard. 799 F.3d at 245. And other dictionaries provide different definitions, such as "contrary to laws or conventions, especially in commerce." *American Heritage Dictionary* 1950 (3d ed. 1992).

contract" could not be deemed unfair unless it involved deceptive or fraudulent behavior. 849 F.2d at 1363. The Court rejected that argument, holding that unfairness is determined by reference to the *Unfairness Statement*'s three-prong test, which is "the most precise definition of unfairness articulated by either the Commission or Congress." *Id.* at 1364 (internal quotation marks omitted); *see also Unfairness Statement*, 104 F.T.C. at 1073 ("[u]njustified consumer injury," determined using the three-prong test, "[b]y itself … can be sufficient to warrant a finding of unfairness").

Orkin specifically made clear that unfairness does not require deceptive conduct. 849 F.2d at 1363 (unfairness need not be "moored in the traditional rationales of anticompetitiveness or *deception*"). This is also evident from the plain language of the statute: if unfairness required deception, Congress would not have prohibited "unfair *or deceptive*" conduct. 15 U.S.C. § 45(a)(1). And the Court's holding that a "mere breach of contract" may be unfair shows that egregiousness is not required. Further rejecting the addition of extra-statutory requirements, such as recklessness, *Orkin* also held that unfairness "does not take into account the mental state" of the violator. 849 F.2d at 1368.[18]

[18] Contrary to LabMD's assertion (Br. 26-27), the Commission has never stated that the three prongs of Section 5(n) are insufficient on their own to show unfairness, nor did the Third Circuit require additional showings in *Wyndham*. The court did not resolve the issue, although it rejected the similar argument that unfairness requires "unscrupulous" or "unethical" conduct. *Wyndham*, 799 F.3d at

E. The Commission Based Its Unfairness Finding on Multiple Security Failures That Led to the Breach.

LabMD argues that the Commission improperly considered LabMD's many data security shortcomings because this case relates "only to security for a single file on a single workstation" and only for the specific 11-month period when the 1718 file was exposed on LimeWire. Br. 29. This argument fails because it conflates the *practices* found to be unfair with the specific *harm* that occurred as a result of those practices. The Commission explained at length that it found "LabMD's security *practices* unreasonable" and that its security failures "*resulted in*" the exposure of the 1718 file. *Opinion* 1, 11-16 (emphasis added). Had LabMD "followed proper data security protocols," the Commission determined, "LimeWire never would have been installed … in the first instance, or it would have been discovered and removed." *Opinion* 16. In other words, the exposure of the 1718 file was the culmination of LabMD's unreasonable and unfair practices. That holding was sound.

The Commission identified three major types of failings by LabMD and tied each of them to the breach. First, LabMD failed to adequately monitor and protect its computer network or employ adequate risk assessment tools and security measures, such as intrusion detection systems, file integrity monitoring, and

---

244-245. Other courts have held that the Section 5(n) elements are sufficient to justify a finding of unfairness. *See, e.g.*, *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1155 (9th Cir. 2010) (an unfair act or practice "is one" that satisfies Section 5(n)).

penetration tests. *Opinion* 12-13. The "consequence of these failures by LabMD was that LimeWire ran undetected on the billing manager's computer between 2005 and 2008," even though adequate security measures could have detected the program. *Opinion* 13-14.

Second, LabMD failed to train its employees on data security and privacy. *Opinion* 14. As a result "employees appear not to have understood the risk in using [peer-to-peer] file sharing software." *Id.*

Third, LabMD did not adequately limit or monitor employees' access to patients' information or restrict employee downloads. *Opinion* 14-16. Had LabMD "followed proper data security protocols, LimeWire never would have been installed on the computer used by LabMD's billing manager in the first instance, or it would have been discovered and removed soon after downloading." *Opinion* 16.

Because the Commission's focus was on the lax security *practices* that led to the breach, it properly considered the full range and duration of those practices.

F. HIPAA Does Not Preempt FTC Authority Over Data Security.

LabMD argues that HIPAA impliedly repealed the FTC's unfairness authority in the field of health care data security. Br. 35-38. This argument fails because there is no conflict, or even potential conflict, between HIPAA and the FTC Act.

Implied repeals are disfavored. The Supreme Court made clear long ago that "[w]here there are two acts upon the same subject, effect should be given to both if possible." *Posadas v. Nat'l City Bank*, 296 U.S. 497, 503 (1936). An implied repeal thus will be found only where provisions in the two acts are in "irreconcilable conflict" or where the later act covers the whole subject of the earlier one and is clearly intended as a substitute. *Id.* Congress's intent to repeal must be "clear and manifest." *Id.*; *accord Branch v. Smith*, 538 U.S. 254, 273 (2003). As the D.C. Circuit has explained, rejecting an argument that another statute implicitly limited the FTC's enforcement authority, "we live in an age of overlapping and concurring regulatory jurisdiction." *FTC v. Ken Roberts Co.*, 276 F.3d 583, 593 (D.C. Cir. 2001). Courts therefore "must proceed with the utmost caution before concluding that one agency may not regulate merely because another may." *Id.*

LabMD points to nothing in the text or legislative history of HIPAA remotely suggesting that Congress intended to limit the FTC's unfairness authority. Nor does LabMD identify any conflict in the two regimes. As the Commission found, "nothing in the FTC Act compels LabMD to engage in practices forbidden by HIPAA, or vice versa." *MTD Order* 12-13.[19] Indeed, HHS works hand-in-hand

[19] *Credit Suisse Securities (USA) LLC v. Billing*, 551 U.S. 264 (2007), is inapposite because it involved a "plain repugnancy" between two statutory regimes that is missing here.

with the FTC "to coordinate enforcement actions for violations that implicate both HIPAA and the FTC Act." HHS, *Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules*, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013). In fact, HHS directs companies to FTC guidance documents to understand their HIPAA obligations.[20] And if there is any difference in the security required by the FTC Act and that required by HIPAA, HHS has noted expressly that its HIPAA rules establish "a minimum level of security that covered entities must meet" and that "covered entities may be required by other Federal law to adhere to additional, or more stringent security measures." *Health Insurance Reform: Security Standards*, Final Rule, 68 Fed. Reg. 8334, 8355 (Feb. 20, 2003).

II. LABMD HAD FAIR NOTICE OF ITS OBLIGATION TO TAKE REASONABLE STEPS TO PROTECT SENSITIVE MEDICAL DATA.

LabMD does not dispute that it knew of its duty to implement reasonable data security measures. Nor could it: its vice president of operations testified about the importance of protecting sensitive medical data and the company assured its clients both that security was part of the service it provided and that data would be maintained on secure servers. *Opinion* 17-18; Tr. 989; CX0704 at 32-33; CX0718 at 17. Furthermore, the company's compliance manual stressed the importance of keeping patient information "secure" and "private" and recognized that giving

[20] *See* https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es.

"patient information … to an unauthorized recipient is a violation of Federal Law." CX0005 at 4.

Attempting to get around these acknowledgements, LabMD resorts to rhetorical sleight-of-hand, arguing that it was denied fair notice of what it terms "Additional Security Measures" that the Commission supposedly required it to adopt. Of course, the Commission did not hold that LabMD was required to adopt a specific set of "Additional Security Measures"—just that it had to employ *reasonable* security measures. As the Third Circuit held in *Wyndham*, due process does not require a greater level of specificity in data security cases. Fair notice was plainly supplied here in two ways: by the statute itself and by multiple sources of industry guidance.

A. Section 5(n) Provides Fair Notice of the Duty To Act Reasonably, and That Standard Is Not Vague.

Like LabMD, Wyndham also claimed that it lacked "fair notice of the specific cybersecurity standards the company was required to follow" and that the FTC was required to spell out these requirements with "ascertainable certainty." *Wyndham*, 799 F.3d at 249, 252. The Third Circuit rejected those arguments. It held that Wyndham was entitled only to "fair notice of what the statute itself requires" and that Section 5(n) itself supplied that notice. *Id*. at 254. The statute is not "so vague as to be no rule or standard at all" because it informs parties of the cost-benefit inquiry that governs their behavior. *Id*. at 255. And while the

application of Section 5(n) may be unclear in "borderline cases," "under a due process analysis a company is not entitled to such precision as would eliminate all close calls." *Id.* at 256.

This Court's approach to fair notice is consistent with *Wyndham*. The Court has held repeatedly that "a civil statute is unconstitutionally vague"—*i.e.*, that it fails to provide fair notice—"only if it is so indefinite as really to be no rule or standard at all." *Leib v. Hillsborough Cty. Pub. Transp. Comm'n*, 558 F.3d 1301, 1310 (11th Cir. 2009) (internal quotation marks omitted). Thus, to be unconstitutionally vague a law must be "substantially incomprehensible." *Reserve, Ltd. v. Town of Longboat Key*, 17 F.3d 1374, 1378 (11th Cir. 1994). Section 5's unfairness standard, as defined by Section 5(n), is not "substantially incomprehensible." As the Commission has made clear, in the data security context, Section 5(n) simply requires businesses to act reasonably.

A reasonableness standard is not unconstitutionally vague. All businesses know that if they fail to take reasonable precautions they can be held liable under ordinary tort law. Just as LabMD did not need to be told to remove hazards from its workplace, it required no special notice that, having collected highly sensitive medical information entrusted to it by doctors and patients, it had to take reasonable measures to protect that data. LabMD is no more entitled to detailed guidance for data protection before FTC enforcement than it would be before a

lawsuit by private plaintiffs injured by its negligence. Courts routinely impose tort liability for violating uncodified standards of care bounded only by the standard of reasonableness. Yet no one could argue that judgments even in novel tort cases violate fair notice or due process principles.

As the Commission noted (*Opinion* 28-29), duties to act "reasonably" and to follow similarly general standards of conduct are ubiquitous in statutory law as well. For example, restraints of trade under the Sherman Act are assessed under a fact-specific "rule of reason." *See, e.g., Leegin Creative Leather Prods., Inc. v. PSKS, Inc.*, 551 U.S. 877, 885 (2007). For more than a century the Supreme Court has deemed this standard consistent with due process. *See Standard Oil Co. v. United States*, 221 U.S. 1, 69 (1911). Public utility and common carrier regulatory statutes generally require companies to offer "just and reasonable" rates and terms of service. *See, e.g., Verizon Commc'ns, Inc. v. FCC*, 535 U.S. 467, 477 (2002); *Permian Basin Area Rate Cases*, 390 U.S. 747, 754 (1968). Courts regularly enforce and apply these requirements.

LabMD's assertion that due process requires the FTC to specify data security standards with "ascertainable certainty" is wrong. LabMD relies on cases involving monetary penalties, which are subject to a stricter due process test than ordinary economic regulations. *See Cotton States Mut. Ins. Co. v. Anderson*, 749 F.2d 663, 669 & n.9 (11th Cir. 1984); *see also Hoffman Estates v. Flipside,*

Hoffman Estates, Inc., 455 U.S. 489, 498 (1982) (vagueness standards cannot be "mechanically applied" and depend "on the nature of the enactment"). For example, in *Georgia Pacific Corp. v. OSHRC*, 25 F.3d 999 (11th Cir. 1994), the Court held that "statutes and regulations which allow monetary penalties against those who violate them" require ascertainable certainty. *Id.* at 1005. Similarly, in *General Electric Co. v. EPA*, 53 F.3d 1324 (D.C. Cir. 1995), the court required ascertainable certainty "because the agency imposed a fine," but held that no such notice would have been required had the agency "merely required … compl[iance] with its regulations." *Id.* at 1328, 1330. Unlike these statutes, the FTC Act does not authorize civil penalties for a violation of Section 5(n).

LabMD is also wrong that a higher notice standard should apply because the Commission seeks *Chevron* deference for its construction of the injury standards of Section 5(n). Br. 43. The question here is whether LabMD had fair notice of the standard of conduct that governed its data security obligations—not whether it understood the precise contours of what constitutes substantial injury. LabMD certainly knew or should have known that its failure to implement adequate data security measures could cause substantial consumer injury. A reasonable business in LabMD's position would have taken steps to avoid such injury; LabMD did not.

Several of LabMD's *amici* make the related claim that the Commission can satisfy due process only if it promulgates specific rules governing data security.

See NFIB Br. 25; Chamber of Commerce Br. 10-17. The claim is squarely foreclosed by *SEC v. Chenery*, 332 U.S. 194 (1947), which held that the SEC could develop behavioral standards by adjudication. The Supreme Court explained that requiring the issuance of rules "would make the administrative process inflexible and incapable of dealing with many of the specialized problems which arise." *Id.* at 202. The choice whether to proceed by rulemaking or adjudication thus lies "in the informed discretion of the administrative agency." *Id.* at 203. The Court reaffirmed these principles in *NLRB v. Bell Aerospace Co.*, holding that an agency "is not precluded from announcing new principles in an adjudicating proceeding." 416 U.S. 267, 294 (1974). Applying those principles, this Court has held that due process does not require agencies to develop policies through rulemaking rather than adjudication. *RTC Transp., Inc. v. ICC*, 731 F.2d 1502, 1505-1506 (11th Cir. 1984).

Like *Chenery*, data-security cases pose questions "so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule." 332 U.S. at 202-203. Data-security risks and standards evolve constantly and vary based on a business's size and the type of data it maintains. *See MTD Order* 14. The FTC therefore "must retain power to deal with [such] problems on a case-by-case basis if the administrative process is to be effective." *Chenery*, 332 U.S. at 203.

B. LabMD Had Substantial Guidance on Reasonable Data Security Measures.

As we have shown, the Commission was not required to spell out in advance a specific set of data security standards for LabMD to follow. Nonetheless, the Commission did provide LabMD (and other businesses) with substantial guidance on reasonable data security measures. As in *Wyndham*, these "additional considerations reinforce the conclusion" that LabMD had fair notice of what Section 5 required. 799 F.3d at 256.

First, the Commission has provided written guidance. In 2007, before the 1718 file was exposed, the Commission published *Protecting Personal Information: A Guide for Business* ("*Business Guide*").[21] The *Business Guide* warns that "the Federal Trade Commission Act may require you to provide reasonable security" (at 5), and cautions against many of the security lapses that led to the release of the 1718 file. It advises using a "properly configured" firewall (at 14), implementing "an intrusion detection system" (at 15), "[m]aintain[ing] central log files of security related information to monitor activity on your network so that you can spot and respond to attacks" (at 15) and monitoring network traffic (at 16). It also emphasizes (at 16-18) the importance of employee training, limiting

[21] For the Court's convenience, we have attached the 2007 version of the *Business Guide* to this brief.

employee access to sensitive information and creating a "culture of security." LabMD did none of this.

LabMD argues that the *Business Guide* does not require companies to engage in any particular security practice and points to Wyndham's statement that the Guide does not provide "ascertainable certainty." Br. 42. But as *Wyndham* explains, "that is not the relevant question." 799 F.3d at 256 n.21. In fact, the Third Circuit relied on the *Business Guide*, noting that it "counsel[s] against many of the specific practices" alleged in that case by the FTC. 799 F.3d at 256.

Second, the Commission provides guidance to the public on reasonable data security through its complaints and consent decrees. Such documents are not legally binding on third parties, but they are published on the FTC's website and in the *Federal Register*, and they reveal the types of security failures the agency deems unreasonable. *See Opinion* 30 n.81 (citing cases). Again, the Third Circuit found these materials relevant in *Wyndham*, noting that courts "regularly consider materials that are neither regulations nor adjudications on the merits" in addressing due process challenges. 799 F.3d at 257.

Finally, other government agencies have also published guidelines that companies use to determine what data security practices are reasonable under their circumstances. For example, the National Institute of Standards and Technology published a risk-management guide in 2002 that sets out risk assessment and

mitigation practices, including the use of cost and benefit analysis to identify security practices that are reasonable under the circumstances. CX0740 at 31 & n.25; CX0400 at 10, 36-38, 44-46. Similarly, the Centers for Medicare and Medicaid Services published a guide in 2005 specifically for companies subject to HIPAA (like LabMD), incorporating the same risk management principles. CX0740 at 31-32 & n.26. This guidance was available to LabMD long before its security failures led to exposure of patient data. Armed with all of this information, a company in LabMD's position would have known how to implement reasonable security measures.

III. SUBSTANTIAL EVIDENCE SUPPORTS THE COMMISSION'S DECISION.

Almost as an afterthought to its erroneous legal arguments, LabMD raises several factual challenges, also baseless, to the Commission's decision.

First, LabMD rehashes its claims that the Commission lacked record evidence quantifying both the "percentage probability" of substantial injury and "the dollar magnitude" of the likely injury. Br. 44-45. As discussed at pages 38-39 above, the 1993 Senate Report and *International Harvester* expressly rejected any such requirement. The Commission's finding of a "high likelihood of harm" from exposure of the 1718 file was amply supported by evidence that the Gnutella network had 2 to 5 million users at any given time, that malicious users commonly

search peer-to-peer networks, and that the 1718 file could have been discovered through a variety of ordinary search techniques. *Opinion* 21-22.

LabMD next asserts that the Commission "ignored" evidence showing that LabMD had adequate data security. Br. 45-46. But under the substantial evidence standard, the Court "will reverse [administrative] findings only when the record *compels* a reversal." *DeKalb County v. DOL*, 812 F.3d 1015, 1020 (11th Cir. 2016) (emphasis added). LabMD has not even attempted to make that showing. In any case, the Commission addressed the evidence that LabMD claims was ignored. *Compare Opinion* 2 n.4, 13 n.35, 15 nn.43-44, 16 n.50 (citing CX0001, CX0443, CX0447, CX0733) *with* Br. 45-46 & nn.19-25 (citing the same exhibits). The Commission did not ignore LabMD's policy manual; it found that LabMD failed to follow the manual—and that LabMD would have detected the installation of LimeWire if it had done so. *Opinion* 16 & n.50. Similarly, the Commission recognized that LabMD's Compliance Manual mandated in-house privacy and data security training, but found that LabMD failed to provide that training. *Opinion* 14 & nn.39-41. Nor did the Commission ignore LabMD's antivirus tools; it found they were used ineffectively *Opinion* 13 & nn.29, 30. Neither did the Commission ignore LabMD's expert testimony regarding network security, configuration, and firewalls; it considered and rejected the expert's opinion as "speculation." *Opinion*

13 & n.33. In short, the Commission considered LabMD's evidence but found it woefully insufficient to demonstrate reasonable security.

LabMD also complains that the Commission improperly relied on testimony from employees not employed by LabMD during the "Relevant Period"—a made-up term which LabMD defines as the 11 months when the 1718 file was exposed to the world. But as discussed at pages 41-42 above, LabMD's unfair practices were not confined to that time period; LabMD's culture of lax security, which led to the release of the file, lasted from 2005 through at least 2010. Furthermore, absent contrary evidence, the Commission could reasonably infer that security failures existing before or after the release of the 1718 file also existed during that time period. LabMD also complains that the Commission relied on investigational hearing testimony of former LabMD employees. But FTC rules permit the use of such testimony as evidence so long as it is "relevant, material, and bears satisfactory indicia of reliability so that its use is fair"—a standard amply met here—and prohibit exclusion "solely on the ground that they are or contain hearsay." 16 C.F.R. § 3.43(b).

Finally, LabMD contends that the Commission cited no evidence that additional employee training, access controls, or file integrity monitoring would have reduced the exposure risk of the 1718 file. Br. 47. But the Commission, like any trier of fact, is permitted to draw "reasonable inferences" from the evidence.

E.g., *Equifax Inc. v. FTC*, 678 F.2d 1047, 1051-1052 (11th Cir. 1982). LabMD cannot reasonably dispute that if employees had been trained about data security risks, including the importance of safeguarding sensitive medical information and the dangers of peer-to-peer file sharing, or if they were prevented from installing unauthorized software on their computers, the data breach would never have occurred. Likewise, had LabMD made some effort to monitor its systems for intrusions, the breach could have been detected. LabMD offers no basis for this Court to second-guess those inferences.

IV. THE COMMISSION'S REMEDY IS PROPER.

The Commission "has wide discretion" in choosing remedies for violations of the FTC Act, and "courts will not interfere except where the remedy selected has no reasonable relation to the unlawful practices found to exist." *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952) (internal quotation marks omitted). Further, the Commission "is not limited to prohibiting the illegal practice in the precise form in which it is found to have existed in the past." *Id.* (same). "[T]hose caught violating the Act must expect some fencing in." *FTC v. National Lead Co.*, 352 U.S. 419, 431 (1957). These principles foreclose LabMD's challenges to the Commission's remedy.

A. The Commission Had Power To Enter a Remedial Order.

LabMD argues that the Commission could not properly issue a cease-and-desist order because the company "discontinued" its illegal conduct. Br. 48-49. It first argues that it cured the security problem by removing LimeWire from the billing manager's computer. The argument rests on the false premise that LabMD's illegal conduct was simply installing LimeWire, rather than the overall failure to implement adequate data security practices. Merely removing the computer program that caused the breach did not suffice to address the lax security problems identified by the Commission.

LabMD next asserts that its voluntary decision to discontinue its business stripped the Commission of power to act. But "discontinuance of an unlawful practice … does not necessarily preclude the issuance of a cease and desist order." *Marlene's, Inc. v. FTC*, 216 F.2d 556, 559 (7th Cir. 1954). "Courts properly leave to the Commission's non-abusive discretion the question whether the public interest requires the protection of an order in cases where unlawful practices have been discontinued." *Cotherman v. FTC*, 417 F.2d 587, 594 (5th Cir. 1969).

The Commission properly exercised its discretion here. It found that LabMD could resume its business, as its owner testified that he would try to do. *Opinion* 36; Tr. 1052-1054. LabMD was highly profitable, and even now it remains incorporated and has retained patient data for 750,000 people, which it

plans to retain for some indefinite period. *See Opinion* 36. LabMD may now deny that it intends to resume business, but its owner testified to the contrary, there is no bar to resumption, and "the Commission is not bound simply by the promises of the petitioners." *Cotherman*, 417 F.2d at 595 (internal quotation marks omitted); *see also Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 189 (2000) (voluntary cessation of operations cannot moot a case unless it is "absolutely clear that the allegedly wrongful behavior could not reasonably be expected to recur").

B. The Commission Ordered Appropriate Relief.

LabMD asserts that by directing LabMD to notify victims of the data breach, the Commission improperly awarded "affirmative relief"— *i.e.*, something other than an order to cease and desist from an unlawful practice. Br. 49-50. But it is settled that the Commission's remedial authority includes the power to order some affirmative relief. For example, the Commission may direct a false advertiser to affirmatively engage in corrective advertising where "necessary to dissipate the effects" of the phony claims. *Warner-Lambert Co. v. FTC*, 562 F.2d 749, 769 (D.C. Cir. 1977). "Orders requiring affirmative disclosures and corrective advertising are clearly within the agency's power." *Southwest Sunsites v. FTC*, 785 F.2d 1431, 1439 (9th Cir. 1986); *accord Amrep Corp. v. FTC*, 768 F.2d 1171, 1180 (10th Cir. 1985). Here, the Commission's order that LabMD notify

consumers that their sensitive information was exposed is necessary to ameliorate the effects of LabMD's conduct. Without knowing that their medical data was exposed, victims do not know they may need to protect themselves from malicious use of their information.

LabMD's cases are inapposite because they do not involve orders that were limited to notice. In *Heater v. FTC*, the court held that the FTC could not order the respondent in an administrative adjudication to *refund money* obtained through practices the Commission held illegal. 503 F.2d 321, 321-322 (9th Cir. 1974). *Congoleum Industries, Inc. v. CPSC* overturned a *recall* of unsafe products. 602 F.2d 220, 226 (9th Cir. 1979); *see also Barrett Carpet Mills, Inc. v. CPSC*, 635 F.2d 299 (4th Cir. 1980) (same). Logically, notice to consumers that their personal data has been compromised is far more akin to corrective advertising than to retrospective redress. It simply gives consumers information they need to make informed choices to protect themselves and is well within the Commission's discretion.

C. The Order Is Not Vague.

LabMD complains that the Commission's requirement to establish a "reasonably designed" security program without specifying the specific security measures LabMD must use is impermissibly vague. Br. 51-52. Because LabMD

failed to raise this claim before the Commission, it is waived. *See, e.g.*, *Vidiksis v. EPA*, 612 F.3d 1150, 1158 (11th Cir. 2010).

In any case, Courts do not set aside injunctions "unless they are so vague that they have no reasonably specific meaning." *Planetary Motion, Inc. v. Techsplosion, Inc.*, 261 F.3d 1188, 1203 (11th Cir. 2001). The Commission's order is very specific; it directs LabMD to implement a security program that is "reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers by" LabMD or its affiliates. *Order* 2. It sets out detailed requirements for the program, including (1) designation of an employee to coordinate and oversee information security, (2) identification of security risks, (3) design and implementation of safeguards to control those risks, (4) requirements that service providers also maintain appropriate safeguards, and (5) evaluation and adjustment based on testing results, changes in business operations, or other factors that materially affect security."[22]

In other words, the Commission spelled out the standards for LabMD to craft a reasonable security program, while giving LabMD the flexibility to tailor its compliance to fit its business operations as they evolve. *Opinion* 36. "[A]bsolute

[22] Those detailed directions do not resemble the prohibition on all "unreasonable restrictions upon competition" held vague in *Asheville Tobacco Board of Trade, Inc. v. FTC*, 294 F.2d 619, 629 (4th Cir. 1961).

precision is not possible in certain FTC orders," *Bristol-Myers Co. v. FTC*, 738 F.2d 554, 560 (2d Cir. 1984), and was not required here.

V. THERE IS NO BASIS FOR A REMAND.

Section 5(c) authorizes reviewing courts to remand cases to the Commission so that a party can "adduce additional evidence," if the requesting party "show[s] to the satisfaction of the court that such additional evidence is material and that there were reasonable grounds for the failure to adduce such evidence in the proceeding before the Commission." 15 U.S.C. § 45(c). LabMD seeks a remand not to "adduce additional evidence," but to take discovery that it speculates might prove that (1) the FTC "had a hand in" Tiversa's acquisition of the 1718 file or (2) the FTC filed its administrative complaint to retaliate against LabMD's CEO for publishing a book. Although many agency statutes contain the identical remand provision, LabMD cites no case in which any court has ever interpreted this to authorize a remand for *discovery*, let alone this kind of fishing expedition.

In any event, LabMD does not come close to meeting the statutory prerequisites. Information about the FTC's relationship with Tiversa is immaterial. LabMD's theory is that if the FTC directed Tiversa to download the 1718 file, its action would violate the Fourth Amendment, such that the entire case must be suppressed as "fruit of the poisonous tree." That is wrong; the law is clear that the Fourth Amendment does not prohibit the government from downloading files

shared on peer-to-peer networks because there is no reasonable expectation of privacy in such files. *E.g.*, *United States v. Stults*, 575 F.3d 834, 842-843 (8th Cir. 2009) (collecting cases). Even if the FTC had directed Tiversa's action—which it did not—such action would not violate the Fourth Amendment.

Nor has LabMD shown any reasonable ground for its previous failure to adduce evidence on this topic. LabMD's assertion that it was denied discovery on this topic is false; in fact, the ALJ permitted LabMD to take the equivalent of a Rule 30(b)(6) deposition of the FTC's Bureau of Consumer Protection on the issue of "how the FTC came to possess the 1718 file." D72 at 8; RX525; RX532. LabMD also took discovery from Tiversa. To the extent that LabMD contends it was entitled to additional discovery on this issue, it never raised that issue before the full Commission; accordingly, the issue is waived.

LabMD's speculative assertion that the FTC may have filed its complaint as retaliation for statements made in a book by LabMD's CEO is also waived. As the Commission found, LabMD raised the argument only in a single sentence in its post-trial brief, with no supporting evidence. *Opinion* 33 n.35. And LabMD never asked the Commission for further discovery on this issue. In any case, it is absurd on its face. The mere fact that the complaint was issued a few days after the book comes out is meaningless, given that the FTC had already been investigating LabMD for three years and was well on its way to filing a complaint. Absent

"clear evidence to the contrary," the Court must presume that the Commissioners "properly discharged their official duties" in filing a complaint. *Brown v. Plata*, 563 U.S. 493, 575-576 (2011). Moreover, allowing discovery on such a speculative claim would allow any target of an FTC (or other government) investigation to raise a retaliation claim simply by publicly criticizing the agency before enforcement.

CONCLUSION

The petition should be denied.

Respectfully submitted,

February 9, 2016

DAVID C. SHONKA
Acting General Counsel

JOEL MARCUS
Deputy General Counsel

/s/ Matthew M. Hoffman
MATTHEW M. HOFFMAN
THEODORE (JACK) METZLER
Attorneys

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Of Counsel:
LAURA RIPOSO VANDRUFF
ALAIN SHEER
JARAD BROWN

FEDERAL TRADE COMMISSION
Washington, D.C. 20580

CERTIFICATE OF COMPLIANCE

I certify that the foregoing brief complies with the type-volume requirements of with Fed. R. App. P. 32(a)(7)(B), as modified by the Court's order of February 8, 2017, because it contains 14,278 words. It complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it is prepared in 14-point Times New Roman using Microsoft Word 2010.

February 9, 2016

/s/ Matthew M. Hoffman
Matthew M. Hoffman

CERTIFICATE OF SERVICE

I certify that I filed the foregoing Brief of the Federal Trade Commission with the Clerk of Court using the Court's CM/ECF system on February 9, 2017. All parties will be served by the system. In addition, I caused a copy of the brief to be delivered via overnight mail to counsel for petitioner as described below:

Douglas H. Meal
Ropes & Gray LLP
Prudential Tower
800 Boylston St.
Boston, MA 02199

/s/ Matthew M. Hoffman
Matthew M. Hoffman

STATUTORY ADDENDUM

United States Code, 2015 Edition
Title 15 - COMMERCE AND TRADE
CHAPTER 2 - FEDERAL TRADE COMMISSION; PROMOTION OF EXPORT TRADE AND PREVENTION OF UNFAIR METHODS OF COMPETITION
SUBCHAPTER I - FEDERAL TRADE COMMISSION
Sec. 45 - Unfair methods of competition unlawful; prevention by Commission
From the U.S. Government Publishing Office, www.gpo.gov

§45. Unfair methods of competition unlawful; prevention by Commission

(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade

(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C. 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C. 227(b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

* * *

(b) Proceeding by Commission; modifying and setting aside orders

Whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect and containing a notice of a hearing upon a day and at a place therein fixed at least thirty days after the service of said complaint. The person, partnership, or corporation so complained of shall have the right to appear at the place and time so fixed and show cause why an order should not be entered by the Commission requiring such person, partnership,

or corporation to cease and desist from the violation of the law so charged in said complaint. Any person, partnership, or corporation may make application, and upon good cause shown may be allowed by the Commission to intervene and appear in said proceeding by counsel or in person. The testimony in any such proceeding shall be reduced to writing and filed in the office of the Commission. If upon such hearing the Commission shall be of the opinion that the method of competition or the act or practice in question is prohibited by this subchapter, it shall make a report in writing in which it shall state its findings as to the facts and shall issue and cause to be served on such person, partnership, or corporation an order requiring such person, partnership, or corporation to cease and desist from using such method of competition or such act or practice. Until the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, or, if a petition for review has been filed within such time then until the record in the proceeding has been filed in a court of appeals of the United States, as hereinafter provided, the Commission may at any time, upon such notice and in such manner as it shall deem proper, modify or set aside, in whole or in part, any report or any order made or issued by it under this section. After the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, the Commission may at any time, after notice and opportunity for hearing, reopen and alter, modify, or set aside, in whole or in part any report or order made or issued by it under this section, whenever in the opinion of the Commission conditions of fact or of law have so changed as to require such action or if the public interest shall so require, except that (1) the said person, partnership, or corporation may, within sixty days after service upon him or it of said report or order entered after such a reopening, obtain a review thereof in the appropriate court of appeals of the United States, in the manner provided in subsection (c) of this section; and (2) in the case of an order, the Commission shall reopen any such order to consider whether such order (including any affirmative relief provision contained in such order) should be altered, modified, or set aside, in whole or in part, if the person, partnership, or corporation involved files a request with the Commission which makes a satisfactory showing that changed conditions of law or fact require such order to be altered, modified, or set aside, in whole or in part. The Commission shall determine whether to alter, modify, or set aside any order of the Commission in response to a request made by a person, partnership, or corporation under paragraph [1] (2) not later than 120 days after the date of the filing of such request.

(c) Review of order; rehearing

Any person, partnership, or corporation required by an order of the Commission to cease and desist from using any method of competition or act or practice may obtain a review of such order in the court of appeals of the United States, within any circuit where the method of competition or the act or practice in question was used or where such person, partnership, or corporation resides or carries on business, by filing in the court, within sixty days from the date of the service of such order, a written petition praying that the order of the Commission be set aside. A copy of such petition shall be forthwith transmitted by the clerk of the court to the Commission, and thereupon the Commission shall file in the court the record in the proceeding, as provided in section 2112 of title 28. Upon such filing of the petition the court shall have jurisdiction of the proceeding and of the question determined therein concurrently with the Commission until the filing of the record and shall have power to make and enter a decree affirming, modifying, or setting aside the order of the Commission, and enforcing the same to the extent that such order is affirmed and to issue such writs as are ancillary to its jurisdiction or are necessary in its judgement to prevent injury to the public or to competitors pendente lite. The findings of the Commission as to the facts, if supported by evidence, shall be conclusive. To the extent that the order of the Commission is affirmed, the court shall thereupon issue its own order commanding obedience to the terms of such order of the Commission. If either party shall apply to the court for leave to adduce additional evidence, and shall show to the satisfaction of the court that such additional evidence is material and that there were reasonable grounds for the failure to adduce such evidence in the proceeding before the Commission, the court may order such additional evidence to be taken before the Commission and to be adduced upon the hearing in such manner and upon such terms and conditions as to the court may seem proper. The Commission may modify its findings as to the facts, or make new findings, by reason of the additional evidence so taken, and it shall file such modified or new findings, which, if supported by evidence, shall be conclusive, and its recommendation, if any, for the modification or setting aside of its original order, with the return of such additional evidence. The judgment and decree of the court shall be final, except that the same shall be subject to review by the Supreme Court upon certiorari, as provided in section 1254 of title 28.

*** * ***

(n) Standard of proof; public policy considerations

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.

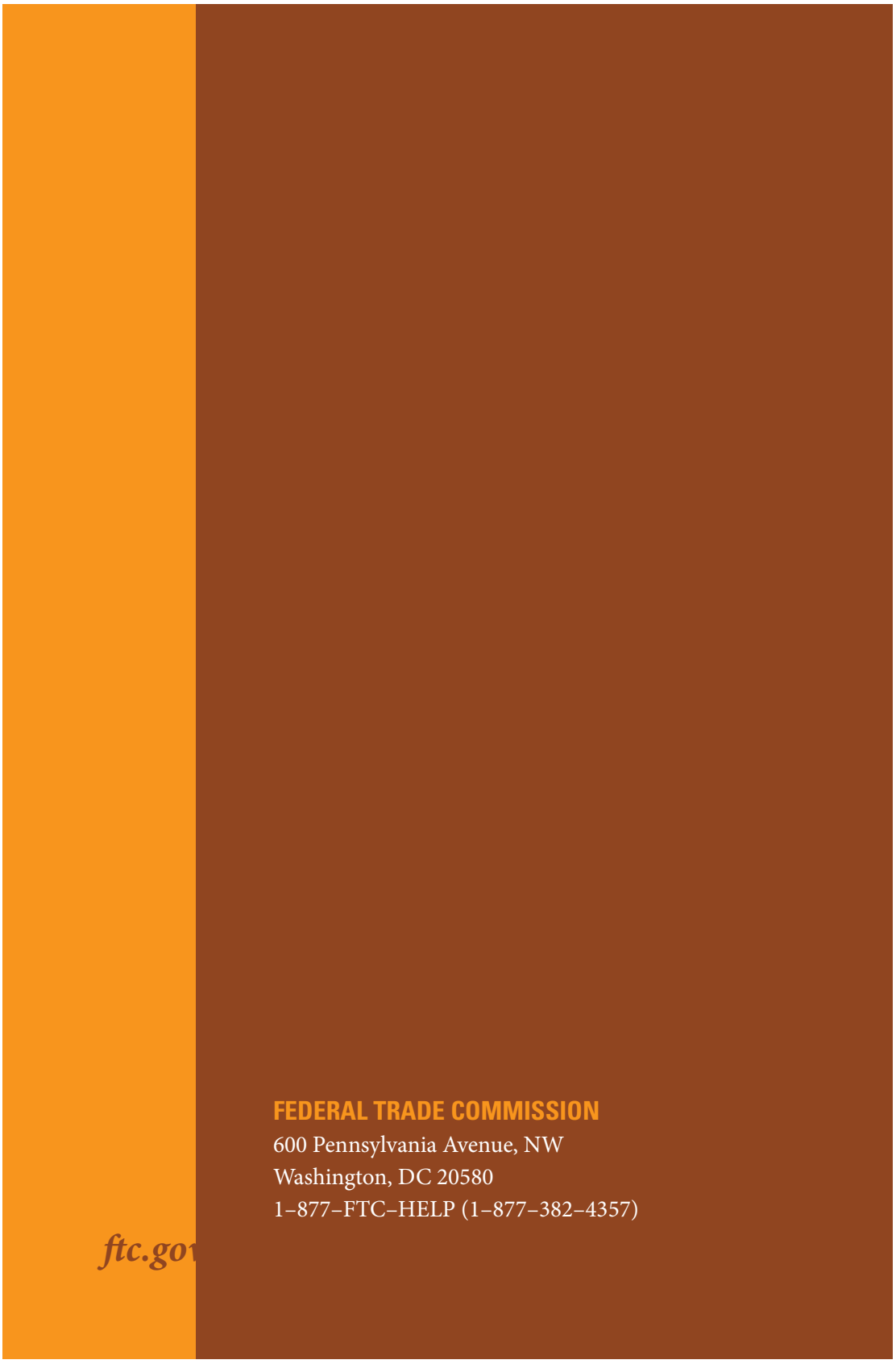
ATTACHMENT

FTC, *Protecting Personal Information: A Guide for Business* (2007)

Protecting PERSONAL INFORMATION

A Guide for Business

FEDERAL TRADE COMMISSION

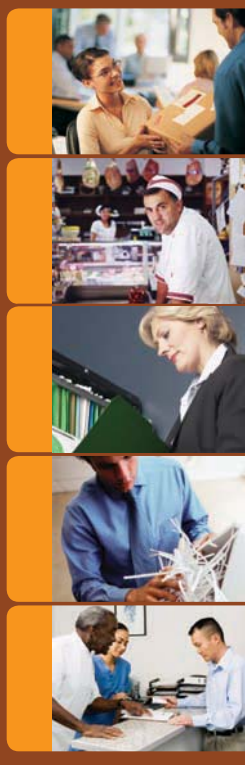

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1–877–FTC–HELP (1–877–382–4357)
ftc.gov

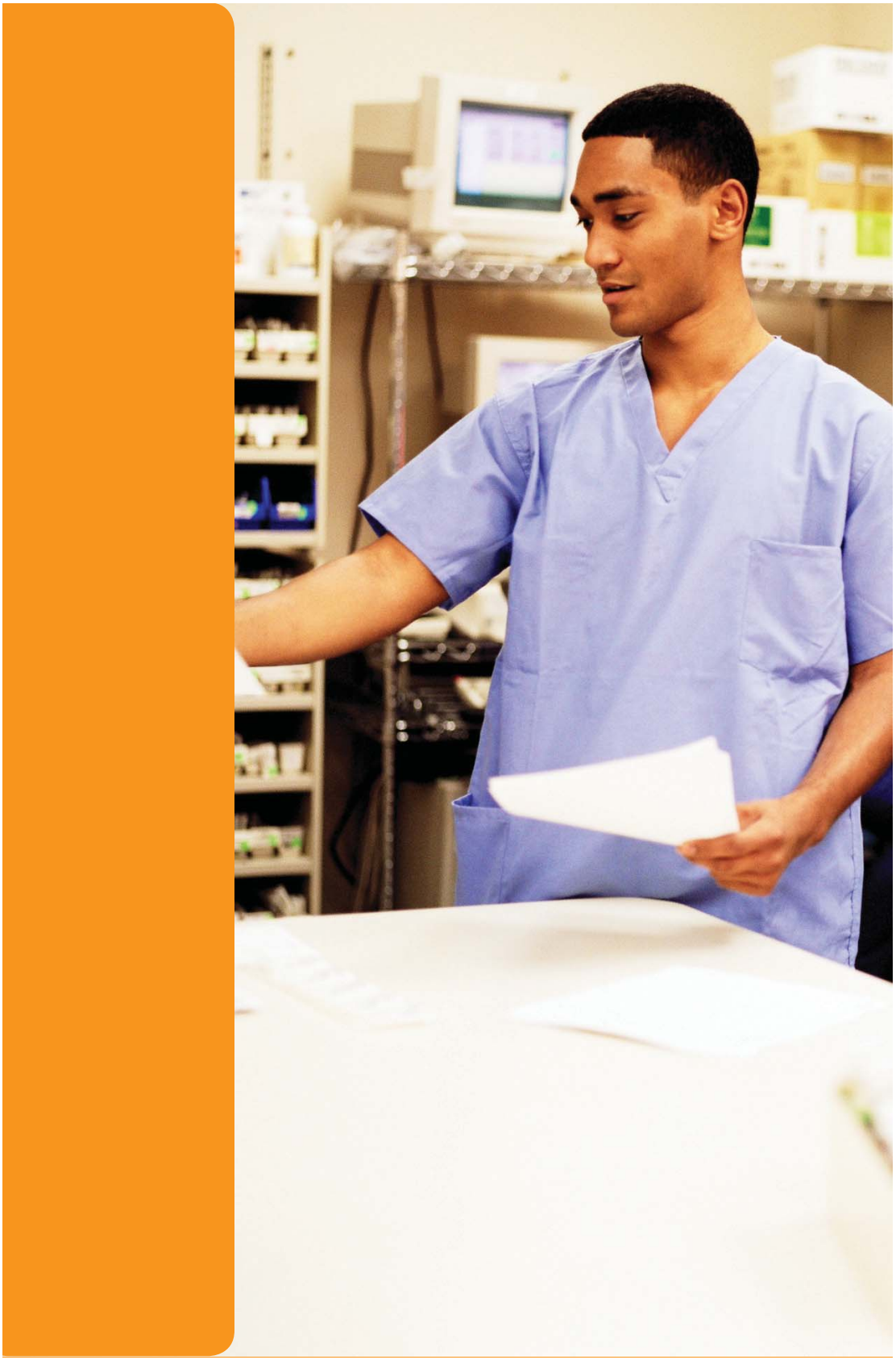
PROTECTING PERSONAL INFORMATION

A Guide for Business

Most companies keep sensitive personal information in their files—names, Social Security numbers, credit card, or other account data—that identifies customers or employees.

This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Given the cost of a security breach—losing your customers' trust and perhaps even defending yourself against a lawsuit—safeguarding personal information is just plain good business.





A sound data security plan is built on **5 key principles:**

1. **Take stock.** Know what personal information you have in your files and on your computers.

2. **Scale down.** Keep only what you need for your business.

3. **Lock it.** Protect the information that you keep.

4. **Pitch it.** Properly dispose of what you no longer need.

5. **Plan ahead.** Create a plan to respond to security incidents.

Use the checklists on the following pages to see how your company's practices measure up—and where changes are necessary.

1. TAKE STOCK. Know what personal information you have in your files and on your computers.

Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities. You can determine the best ways to secure the information only after you've traced how it flows.

- Inventory all computers, laptops, flash drives, disks, home computers, and other equipment to find out where your company stores sensitive data. Also inventory the information you have by type and location. Your file cabinets and computer systems are a start, but remember: your business receives personal information in a number of ways—through websites, from contractors, from call centers, and the like. What about information saved on laptops, employees' home computers, flash drives, and cell phones? No inventory is complete until you check everywhere sensitive data might be stored.
- Track personal information through your business by talking with your sales department, information technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of:

- ***Who sends sensitive personal information to your business.*** Do you get it from customers? Credit card companies? Banks or other financial institutions? Credit bureaus? Other businesses?
- ***How your business receives personal information.*** Does it come to your business through a website? By email? Through the mail? Is it transmitted through cash registers in stores?
- ***What kind of information you collect at each entry point.*** Do you get credit card information online? Does your accounting department keep information about customers' checking accounts?
- ***Where you keep the information you collect at each entry point.*** Is it in a central computer database? On individual laptops? On disks or tapes? In file cabinets? In branch offices? Do employees have files at home?
- ***Who has—or could have—access to the information.*** Which of your employees has permission to access the information? Could anyone else get a hold of it? What about vendors who supply and update software you use to process credit card transactions? Contractors operating your call center?

- Different types of information present varying risks. Pay particular attention to how you keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft.

SECURITY CHECK

Question:

Are there laws that require my company to keep sensitive data secure?

Answer:

Yes. While you're taking stock of the data in your files, take stock of the law, too. Statutes like the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act may require you to provide reasonable security for sensitive information.

To find out more, visit ***www.ftc.gov/privacy***.

TAKE STOCK.

1

2. SCALE DOWN. Keep only what you need for your business.

If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it only as long as it's necessary.

- Use Social Security numbers only for required and lawful purposes—like reporting employee taxes. Don't use Social Security numbers unnecessarily—for example, as an employee or customer identification number, or because you've always done it.

SECURITY CHECK

Question:

We like to have accurate information about our customers, so we usually create a permanent file about all aspects of their transactions, including the information we collected from the magnetic stripe on their credit cards. Could this practice put their information at risk?

Answer:

Yes. Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not in your system, it can't be stolen by hackers. It's as simple as that.

- Don't keep customer credit card information unless you have a business need for it. For example, don't retain the account number and expiration date unless you have an essential business need to do so. Keeping this information—or keeping it longer than necessary—raises the risk that the information could be used to commit fraud or identity theft.
- Check the default settings on your software that reads customers' credit card numbers and processes the transactions. Sometimes it's preset to keep information permanently. Change the default setting to make sure you're not inadvertently keeping information you don't need.
- If you must keep information for business reasons or to comply with the law, develop a written records retention policy to identify what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when you no longer need it.

3. LOCK IT. Protect the information that you keep.

What's the best way to protect the sensitive personally identifying information you need to keep? It depends on the kind of information and how it's stored. The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers.

PHYSICAL SECURITY

Many data compromises happen the old-fashioned way—through lost or stolen paper documents. Often, the best defense is a locked door or an alert employee.

- Store paper documents or files, as well as CDs, floppy disks, zip drives, tapes, and backups containing personally identifiable information in a locked room or in a locked file cabinet. Limit access to employees with a legitimate business need. Control who has a key, and the number of keys.

- Require that files containing personally identifiable information be kept in locked file cabinets except when an employee is working on the file. Remind employees not to leave sensitive papers out on their desks when they are away from their workstations.
- Require employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building. Tell employees what to do and whom to call if they see an unfamiliar person on the premises.
- If you maintain offsite storage facilities, limit employee access to those with a legitimate business need. Know if and when someone accesses the storage site.
- If you ship sensitive information using outside carriers or contractors, encrypt the information and keep an inventory of the information being shipped. Also use an overnight shipping service that will allow you to track the delivery of your information.

ELECTRONIC SECURITY

Computer security isn't just the realm of your IT staff. Make it your business to understand the vulnerabilities of your computer system, and follow the advice of experts in the field.

General Network Security

- Identify the computers or servers where sensitive personal information is stored.
- Identify all connections to the computers where you store sensitive information. These may include the Internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, and wireless devices like inventory scanners or cell phones.

- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.
- Don't store sensitive consumer data on any computer with an Internet connection unless it's essential for conducting your business.
- Encrypt sensitive information that you send to third parties over public networks (like the Internet), and consider encrypting sensitive information that is stored on your computer network or on disks or portable storage devices used by your employees. Consider also encrypting email transmissions within your business if they contain personally identifying information.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on servers on your network.
- Check expert websites (such as ***www.sans.org***) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems.
- Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- When you receive or transmit credit card information or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.

SECURITY CHECK

Question:

We encrypt financial data customers submit on our website. But once we receive it, we decrypt it and email it over the Internet to our branch offices in regular text. Is there a safer practice?

Answer:

Yes. Regular email is not a secure method for sending sensitive data. The better practice is to encrypt any transmission that contains information that could be used by fraudsters or ID thieves.

- Pay particular attention to the security of your web applications—the software used to give information to visitors to your website and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks. In one variation called an "injection attack," a hacker inserts malicious commands into what looks like a legitimate request for information. Once in your system, hackers transfer sensitive information from your network to their computers. Relatively simple defenses against these attacks are available from a variety of sources.

Password Management

- Control access to sensitive information by requiring that employees use "strong" passwords. Tech security experts say the longer the password, the better. Because simple passwords—like common dictionary words—can be guessed easily, insist that employees choose passwords with a mix of letters, numbers, and characters. Require an employee's user name and password to be different, and require frequent changes in passwords.
- Explain to employees why it's against company policy to share their passwords or post them near their workstations.
- Use password-activated screen savers to lock employee computers after a period of inactivity.
- Lock out users who don't enter the correct password within a designated number of log-on attempts.

SECURITY CHECK

Question:

Our account staff needs access to our database of customer financial information. To make it easier to remember, we just use our company name as the password. Could that create a security problem?

Answer:

Yes. Hackers will first try words like "password," your company name, the software's default password, and other easy-to-guess choices. They'll also use programs that run through common English words and dates. To make it harder for them to crack your system, select strong passwords—the longer, the better—that use a combination of letters, symbols, and numbers. And change passwords often.

- Warn employees about possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.
- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
- Caution employees against transmitting sensitive personally identifying data—Social Security numbers, passwords, account information—via email. Unencrypted email is not a secure way to transmit any information.

Laptop Security

- Restrict the use of laptops to those employees who need them to perform their jobs.
- Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a "wiping" program that overwrites data on the laptop. Deleting files using standard keyboard commands isn't sufficient because data may remain on the laptop's hard drive. Wiping programs are available at most office supply stores.
- Require employees to store laptops in a secure place. Even when laptops are in use, consider using cords and locks to secure laptops to employees' desks.

- Consider allowing laptop users only to access sensitive information, but not to store the information on their laptops. Under this approach, the information is stored on a secure central computer and the laptops function as terminals that display information from the central computer, but do not store it. The information could be further protected by requiring the use of a token, "smart card," thumb print, or other biometric—as well as a password—to access the central computer.
- If a laptop contains sensitive data, encrypt it and configure it so users can't download any software or change the security settings without approval from your IT specialists. Consider adding an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet.
- Train employees to be mindful of security when they're on the road. They should never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security. If someone must leave a laptop in a car, it should be locked in a trunk. Everyone who goes through airport security should keep an eye on their laptop as it goes on the belt.

Firewalls

- Use a firewall to protect your computer from hacker attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.
- Determine whether you should install a "border" firewall where your network connects to the Internet. A border firewall separates your network from the Internet and may prevent an attacker from gaining access to a computer on the network where you store sensitive information. Set "access controls"—settings that determine who gets through the firewall and what they will be allowed to see—to allow only trusted employees with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, review them periodically.
- If some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information.

Wireless and Remote Access

- Determine if you use wireless devices like inventory scanners or cell phones to connect to your computer network or to transmit sensitive information.
- If you do, consider limiting who can use a wireless connection to access your computer network. You can make it harder for an intruder to access the network by limiting the wireless devices that can connect to your network.
- Better still, consider encryption to make it more difficult for an intruder to read the content. Encrypting transmissions from wireless devices to your computer network may prevent an intruder from gaining access through a process called "spoofing"—impersonating one of your computers to get access to your network.
- Consider using encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases.

Detecting Breaches

- To detect network breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.
- Maintain central log files of security-related information to monitor activity on your network so that you can spot and respond to attacks. If there is an attack on your network, the log will provide information that can identify the computers that have been compromised.

- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from your system to an unknown user. If large amounts of information are being transmitted from your network, investigate to make sure the transmission is authorized.
- Have in place and implement a breach response plan. See pages 22–23 for more information.

EMPLOYEE TRAINING

Your data security plan may look great on paper, but it's only as strong as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance you place on meaningful data security practices. A well-trained workforce is the best defense against identity theft and data breaches.

- Check references or do background checks before hiring employees who will have access to sensitive data.
- Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by your company's data security plan is an essential part of their duties. Regularly remind employees of your company's policy—and any legal requirement—to keep customer information secure and confidential.
- Know which employees have access to consumers' sensitive personally identifying information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a "need to know."
- Have a procedure in place for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out routine.

SECURITY CHECK

Question:

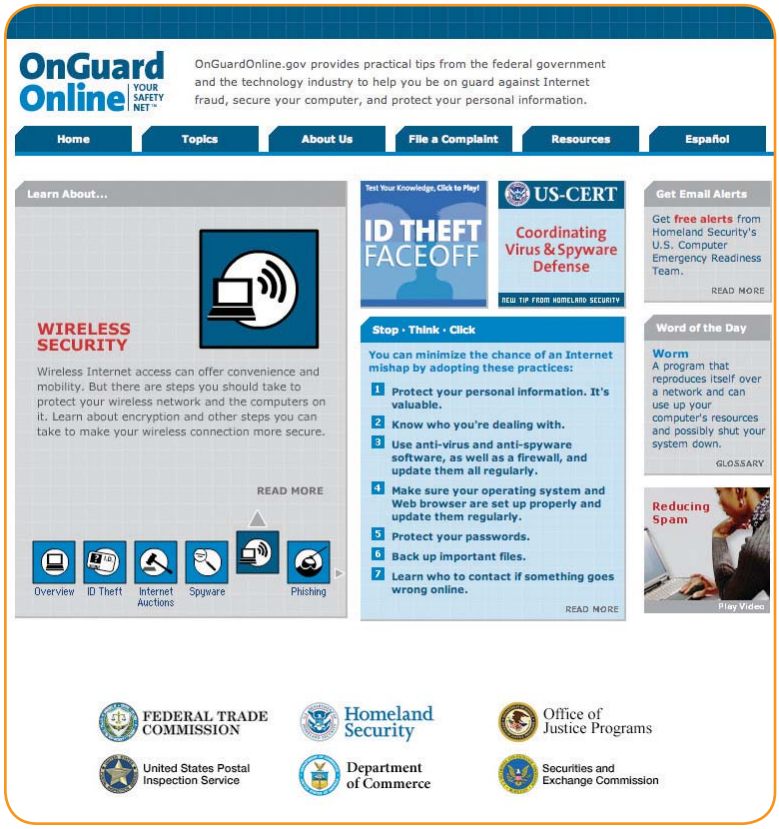
I'm not really a "tech" type. Are there steps our computer people can take to protect our system from common hack attacks?

Answer:

Yes. There are relatively simple fixes to protect your computers from some of the most common vulnerabilities. For example, a threat called an "SQL injection attack" can give fraudsters access to sensitive data on your system, but can be thwarted with a simple change to your computer. Bookmark the websites of groups like the Open Web Application Security Project, ***www.owasp.org***, or SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities, ***www.sans.org/top20***, for up-to-date information on the latest threats—and fixes. And check with your software vendors for patches that address new vulnerabilities.

- Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. Make sure training includes employees at satellite offices, temporary help, and seasonal workers. If employees don't attend, consider blocking their access to the network.
- Train employees to recognize security threats. Tell them how to report suspicious activity and publicly reward employees who alert you to vulnerabilities.

- Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate. Make sure your policies cover employees who telecommute or access sensitive data from home or an offsite location.
- Warn employees about phone phishing. Train them to be suspicious of unknown callers claiming to need account numbers to process an order or asking for customer or employee contact information. Make it office policy to double-check by contacting the company using a phone number you know is genuine.
- Require employees to notify you immediately if there is a potential security breach, such as a lost or stolen laptop.
- Impose disciplinary measures for security policy violations.
- For computer security tips, tutorials, and quizzes for everyone on your staff, visit ***www.OnGuardOnline.gov***.



SECURITY PRACTICES OF CONTRACTORS AND SERVICE PROVIDERS

Your company's security practices depend on the people who implement them, including contractors and service providers.

- Before you outsource any of your business functions—payroll, web hosting, customer call center operations, data processing, or the like—investigate the company's data security practices and compare their standards to yours. If possible, visit their facilities.
- Address security issues for the type of data your service providers handle in your contract with them.
- Insist that your service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of your data.

4. PITCH IT. Properly dispose of what you no longer need.

What looks like a sack of trash to you can be a gold mine for an identity thief. Leaving credit card receipts or papers or CDs with personally identifying information in a dumpster facilitates fraud and exposes consumers to the risk of identity theft. By properly disposing of sensitive information, you ensure that it cannot be read or reconstructed.

- Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to—or use of—personally identifying information. Reasonable measures for your operation are based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

SECURITY CHECK

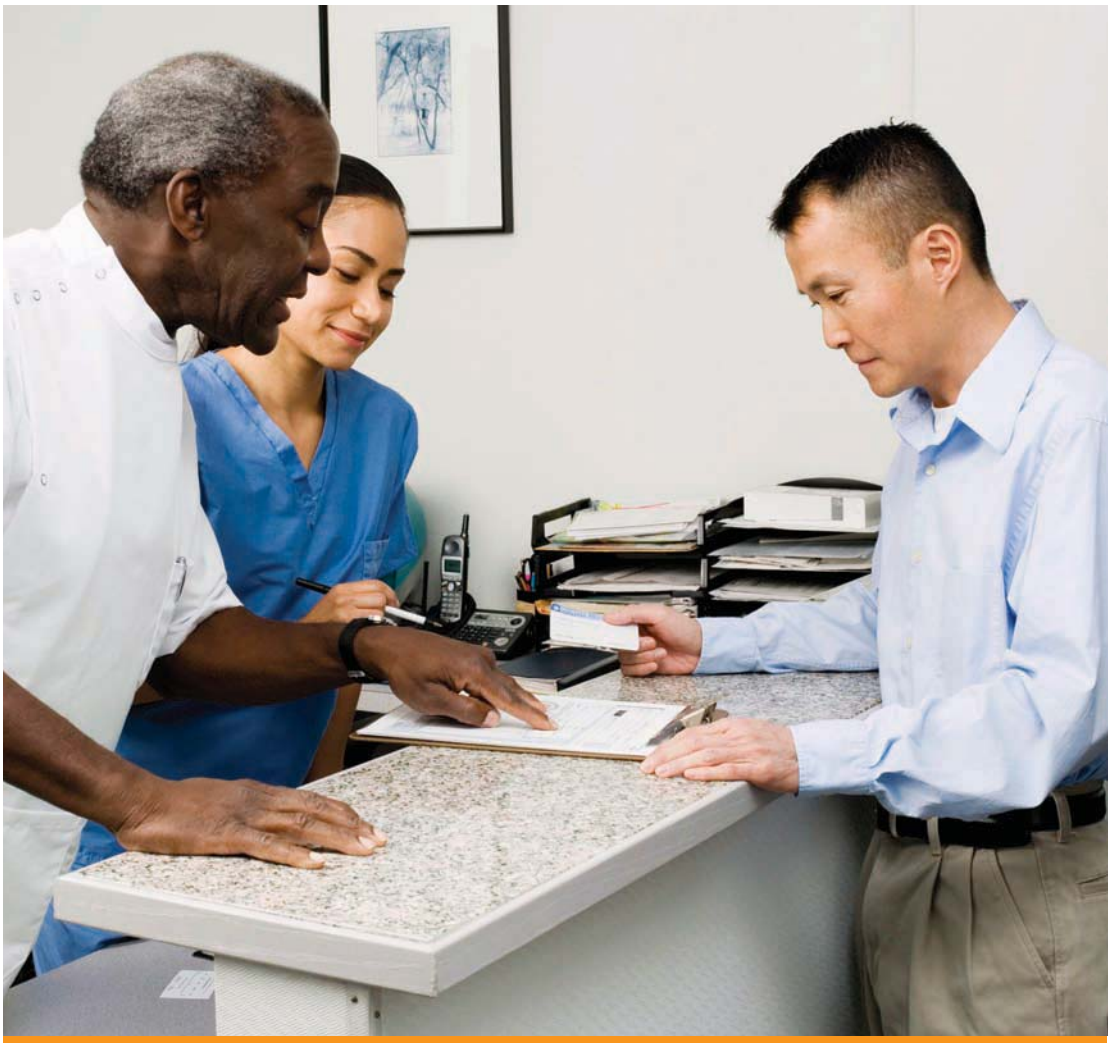
Question:

My company collects credit applications from customers. The form requires them to give us lots of financial information. Once we're finished with the applications, we're careful to throw them away. Is that sufficient?

Answer:

No. Have a policy in place to ensure that sensitive paperwork is unreadable before you throw it away. Burn it, shred it, or pulverize it to make sure identity thieves can't steal it from your trash.

- Effectively dispose of paper records by shredding, burning, or pulverizing them before discarding. Make shredders available throughout the workplace, including next to the photocopier.
- When disposing of old computers and portable storage devices, use wipe utility programs. They're inexpensive and can provide better results by overwriting the entire hard drive so that the files are no longer recoverable. Deleting files using the keyboard or mouse commands usually isn't sufficient because the files may continue to exist on the computer's hard drive and could be retrieved easily.
- Make sure employees who work from home follow the same procedures for disposing of sensitive documents and old computers and portable storage devices.
- If you use consumer credit reports for a business purpose, you may be subject to the FTC's Disposal Rule. For more information, see *Disposing of Consumer Report Information? New Rule Tells How* at ***www.ftc.gov/privacy*** (click on Credit Reporting, Business Guidance).



5. PLAN AHEAD. Create a plan for responding to security incidents.

Taking steps to protect data in your possession can go a long way toward preventing a security breach. Nevertheless, breaches can happen. Here's how you can reduce the impact on your business, your employees, and your customers:

- Have a plan in place to respond to security incidents. Designate a senior member of your staff to coordinate and implement the response plan.
- If a computer is compromised, disconnect it immediately from the Internet.

SECURITY CHECK

Question:

I own a small business. Aren't these precautions going to cost me a mint to implement?

Answer:

No. There's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers. Some of the most effective security measures—using strong passwords, locking up sensitive paperwork, training your staff, etc.—will cost you next to nothing and you'll find free or low-cost security tools at non-profit websites dedicated to data security. Furthermore, it's cheaper in the long run to invest in better data security than to lose the goodwill of your customers, defend yourself in legal actions, and face other possible consequences of a data breach.

- Investigate security incidents immediately and take steps to close off existing vulnerabilities or threats to personal information.
- Consider whom to notify in the event of an incident, both inside and outside your organization. You may need to notify consumers, law enforcement, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, many states and the federal bank regulatory agencies have laws or guidelines addressing data breaches. Consult your attorney.

5

ADDITIONAL RESOURCES

These websites and publications have more information on securing sensitive data:

- National Institute of Standards and Technology (NIST)'s Computer Security Resource Center
  www.csrc.nist.gov
- NIST's Risk Management Guide for Information Technology Systems
  www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Department of Homeland Security's National Strategy to Secure Cyberspace
  www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
- SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities
  www.sans.org/top20
- United States Computer Emergency Readiness Team (US-CERT)
  www.us-cert.gov
- Carnegie Mellon Software Engineering Institute's CERT Coordination Center
  www.cert.org/other_sources
- Center for Internet Security (CIS)
  www.cisecurity.org
- The Open Web Application Security Project
  www.owasp.org
- Institute for Security Technology Studies
  www.ists.dartmouth.edu
- OnGuard Online
  www.OnGuardOnline.gov

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free 1–877–FTC-HELP (1–877–382–4357); TTY: 1–866–653–4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Opportunity to Comment

The Small Business and Agriculture Regulatory Enforcement Ombudsman and 10 Regional Fairness Boards collect comments from small business about federal enforcement actions. Each year, the Ombudsman evaluates enforcement activities and rates each agency's responsiveness to small business. To comment on FTC actions, call 1–888–734–3247.

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1–877–FTC–HELP (1–877–382–4357)

ftc.gov