CHAPTER 10

DATA SECURITY

CHAPTER OUTLINE

A. INTRODUCTION

Consumers at Risk. In testimony to Congress in 2014, Edith Ramirez, the Chairwoman of the Federal Trade Commissioner, bluntly stated, "Consumers' data is at risk."[1] She also noted the critical importance of data security to consumers: "If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud, identity theft, and other harm, along with a potential loss of consumer confidence in the marketplace." Data security is more crucial than ever before, but more data breaches are taking places. The leaks involve Social Security numbers, payment card data, account passwords, health data, information about children, and many other types of personal information.

A data breach involving Target made worldwide headlines in 2013 and 2014. According to subsequent investigations, hackers using credentials from a HVAC vendor of the retailer entered into Target's computer network.[2] Once inside, the hackers installed malware that allowed them to steal credit card numbers from cashier stations in Target stores. The stolen information was temporarily stored within Target servers then sent to a hijacked "staging point" in the United States and then onward to the hackers in Russia. Target was obliged to announce the

[1] Edith Ramirez, Prepared Statement of the Federal Trade Commission on Data Breach on the Rise: Protecting Personal Information from Harm, Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate (Apr. 2, 2014).

[2] Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Business Week (Mar. 13, 2014).

breach at perhaps the worst point possible in its sales year: December 15. By this point, 40 million credit card numbers had been stolen from the retailer. In August 2014, Target announced that it expected $148 million in expenses related to the breach.[3]

The problem of data security goes far beyond Target, and the dimensions of the problem are staggering. According to a Pew Research Poll from 2014, 18 percent of all online Americans report having had personal information stolen.[4] Separate studies by the Javelin Strategy and Research Group and by LexisNexis estimate that one-fourth of records involved in data breaches are used for fraudulent purposes, such as identity theft.[5] For a snapshot of the extent of data breaches today, two state reports are highly useful. Both California and New York require reporting of data breach notifications to state officials in their respective jurisdictions. In 2013, the California Department of Justice (DOJ) published its first review of these reports.[6] In 2012, it received reports of 131 data breaches, which put more than 2.5 million Californians at risk. Had the data in question only been encrypted, more than 1.4 million Californians would not have been put at risk and 28 percent of the breaches would not have required notification. The industries that reported the most data breaches in the state were the retail industry, followed by finance and insurance. Finally, more than half of the breaches involved Social Security numbers, which, according to the California DOJ, "pose the greatest risk of the most serious types of identity theft."

While California only mandated the filing of notices with state officials in 2011 and received its first reports in 2012, New York has been receiving breach notification reports since 2006. Its 2014 report was therefore able to analyze eight years of data breach notifications.[7] Between 2006 and 2013, the number of reported data security breaches more than tripled. As the Attorney General (AG) of New York, observes: "Over 22 million personal records have been exposed since 2006, jeopardizing the financial health and well-being of countless New Yorkers and costing the public and private sectors in New York — and around the world — billions of dollars." The report estimates the cost of data breaches for 2013 alone at more than $1.37 billion. It also found that five of the ten largest breaches affecting New York residents occurred in the past three years. Moreover, "mega-breaches" were responsible for nearly 80 percent of the personal records exposed in the state. Specifically, the New York State AG found that 28 mega-breaches exposed approximately 18.2 million personal records of New Yorkers.

[3] Michael Calia, *Target Lowers Outlook on Retail Softness, Data Breach Expenses*, Wall St. J. (Aug. 5, 2014).

[4] Mary Madden, Pew Research Center, More online Americans say they've experienced a personal data breach (Apr. 14, 2014).

[5] Lexis-Nexis True Cost of Fraud Study, Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud 6 (2013).

[6] California Department of Justice, Data Breach Report 2012 (2013).

[7] New York State Attorney General, Information Exposed: Historical Examination of Data Breaches in New York State (2014).

Fines, Settlements, and High Financial Stakes. The stakes for consumers in data breaches are high. This area is equally important for organizations. Writing in *Computer World*, Jay Cline has tallied up the overall enforcement actions and fines for data privacy violations.[8] His conclusion: "Over the last 15 years, security breaches were the most likely to draw a large fine. They accounted for some 35% of the sizable penalties in our database." The top government- imposed fines for security flaws are against ChoicePoint, a database company, for $15 million (2006); LifeLock, an identity theft protection company, for $12 million (2010); CVS Caremark, a pharmacy chain, for $2.25 million (2009). The ChoicePoint settlement was with the FTC; the CVS Caremark settlement was with the U.S. Department of Health of Health and Human Services and the FTC; the LifeLock settlement was with the FTC and a group of 35 state attorneys general. In a tally from FTC Chairwoman Ramirez, this agency alone has settled more than 50 cases with businesses that it charged with failing to provide reasonable protection for the personal information of consumers.

Another reason that data security is a high-risk area for organizations is the threat of class action lawsuits. Data breach class action lawsuits have led to massive financial settlements. For example, in 2014, Sony agreed to a $15 million settlement of a class action lawsuit for the 2011 hacking of its PlayStation Network. The overall cost of cleaning up the breach, which caused a shut-down of the PlayStation Network for several weeks, has been estimated at $171 million. A data breach lawsuit in Florida against Avmed, Inc, a health care company, led to a $3 million settlement in 2013. The Eleventh Circuit's opinion in this case, *Resnick v. Avmed*, is excerpted below. Once the appellate court denied Avmed's motion for summary judgment, the company quickly settled.

B. DATA SECURITY BREACH NOTIFICATION STATUTES

California was the first state to require companies that maintain personal information to notify individuals in the event of a security breach where personal information is leaked or improperly accessed. The California statute was enacted in 2003. Pursuant to SB 1386, codified at Cal. Civ. Code § 1798.82(a):

> Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. . . .

[8] Jay Cline, U.S. takes the gold in doling out privacy fines, Computer World (Feb. 17, 2014).

The California security breach notice provision received national attention after the ChoicePoint data security breach in 2005. At the time, California was the only state with such a law. The security breach occurred because an identity theft crime ring set up fake businesses and then signed up to receive ChoicePoint's data. As a result, personal information, including names, addresses, and Social Security numbers of over 145,000 people, were improperly accessed. Over 700 of these individuals were victimized by some form of identity theft.

The fraud was discovered in October 2004 by ChoicePoint, but victims were not notified until February 2005 to avoid impeding the law enforcement investigation. When news of the breach was announced, it sparked considerable public attention. After angry statements by many state attorneys general and a public outcry, ChoicePoint decided to voluntarily notify all individuals affected by the breach, not just Californians.

Today, 48 states and the District of Columbia have such laws. Alabama and South Dakota are the remaining states without a breach notification law. Data breach notification statutes require governmental agencies and/or private companies to disclose security breaches involving personal information.[9] The resulting laws vary according to the following criteria: (1) the definition of covered information; (2) the trigger for notification; (3) any exceptions to the law's notification requirement; (4) a requirement of notification to a state agency or attorney general; (5) the presence or absence of a substantive requirement for data security; and (6) the presence or absence of a private right of action.[10]

Although the federal government has yet to enact a general federal data breach notification statute, in 2009, Congress enacted a data breach notification requirement for entities regulated by HIPAA as part of the HITECH Act.

The idea of data breach notification, born in California, has grown to achieve international popularity. The EU's ePrivacy Directive, as revised in 2009, requires telecommunication operators and Internet service providers to report "personal data breaches" to the respective national authority. When a breach is likely to adversely affect personal data, affected subscribers must be notified. More broadly, the Proposed General Data Protection Regulation of 2012 contains a requirement of notification of the supervisory authority within 24 hours of a breach. When a breach is likely to affect the privacy of an individual adversely, the data controller must inform this affected party without undue delay. Once enacted, the Data Protection Regulation will be immediately binding on all Member States and extend a breach notification requirement throughout the European Union.

Covered Information. The California data breach statute defines the underlying "notice-triggering information" as "first name or initial and last name" and any of the following list of other data: Social Security number; driver's license number; financial account number plus a password. In a 2013 amendment to the

[9] National Conference of State Legislatures, State Security Breach Notifications Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited July 16, 2008. For an analysis of data security breach laws, see Paul Schwartz & Edward Janger, *Notification of Data Security Breaches*, 105 Mich. L. Rev. 913, 924-25 (2007).

[10] For a chart examining these laws, state by state, see Daniel J. Solove & Paul M. Schwartz, *Privacy Law Fundamentals* 172-74 (2013).

statute, California became the first state to expand this definition to include user names or e-mail addresses in combination with a password or a security question and answer that would permit access to an online account. Florida, Georgia, and other states have followed this approach.

Like California, other states also define personal information as a party's name in conjunction with a list of other elements. For example, Maine has a data elements list that includes a broad savings clause to broaden the law beyond a person's name. Maine extends its data breach law to any of the listed data elements *without* a person's name "if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised."

Trigger for Notification. Most states follow the California approach and rely on the "acquisition" standard for breach notification. These states generally require notification whenever there is a reasonable likelihood that an unauthorized party has "acquired" person information. A minority of states have adopted a higher standard. These states consider whether there is a reasonable likelihood of "misuse" of the information, or "material risk" of harm to the person. The idea is that a breach letter should not be sent to the affected public unless there is a more significant likelihood of harm.

Thus, California's breach notification law requires notification when "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code 17982(a). The California Office of Privacy Protection has issued a white paper with its recommendations regarding notification of security breaches.[11] In the white paper, it lists three factors to be considered, among others, in determining whether unencrypted notice-triggering information has been acquired:

> 1. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device ....
>
> 2. Indications that the information has been downloaded or copied.
>
> 3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Other states have a stricter notification standard, that is, one that is further from the pro-notification side of the continuum than California. These states generally require notification only if "misuse" of a state resident's personal information has occurred or is reasonably likely to occur. States that use a misuse standard include Delaware and Kansas. Other states require a "risk of analysis" finding that misuse is *not* likely to occur. Such states include Maryland, Maine, and New Jersey. Which of these standards do you think is best?

[11] California Office of Privacy Protection, Recommended Practices on Notice of Security Breach Involving Personal Information (Jan. 2012).

Exceptions to Notification. Numerous states provide exceptions to the notification requirement if a risk of harm analysis shows that harm to a consumer will not result. Thus, Michigan does not require notification if the "person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, [one] or more residents." Me. Rev. Stat. tit. 10 § 1348(1)(B) (2014). North Carolina does not consider an acquisition of information a "security breach" if illegal use of the information did not occur or is not reasonably likely to occur, or does not "create[] a material risk of harm to a consumer." N.C. Gen. Stat. § 75-61(14) (2014). The New Jersey exception is for a business that establishes that "misuse of the information is not reasonably possible." N.J. Stat. § 56:8-163(a) (2014).

Florida has recently narrowed its risk analysis against possible misuse. Traditionally, it has not required notification if a data breach "has not and will not result in identity theft or other financial harm to the individual whose personal information has been acquired and accessed." Fla. Stat. § 817.5681(10)(a) (2013) (repealed 2014). However, the Florida Information Protection Act of 2014 (FIPA) requires "appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies" before it can make a "no harm" determination, which it must provide to the Florida Department of Legal Affairs (FDLA). 2014 Fla. Laws ch. 189 § 3(4)(c). Moreover, the amendment requires notification to the FDLA of a breach affecting 500 or more individuals in Florida, without regard to likely harm. This notice is to include key details of the event, and the FDLA is authorized to request copies of the relevant police report, forensic report, and existing security policies of the affected entity.

Notification to State Agency or Attorney General. All the breach notification statutes require notification to the affected party. Writing in 2007, Paul Schwartz and Edward Janger argued that a critical need in the area of data security breaches was for a "coordinated response architecture," which would include a "coordinated response agent" (CRA) to help tailor notice content and supervise the decision whether to give notice.[12] The CRA was to help coordinate actions that companies take after a breach, tailor the content of the notification in light of the nature of the data breach, and help prepare comparative statistical information regarding data security events. Data breach notification laws that require notification to state entities are a strong step towards creation of such a "response architecture." Now states have information about the kinds of breaches that are occurring, whether notification has occurred, and indications of the kinds of potential harms to state residents. Notification also helps state entities decide whether to begin investigations and enforcement actions.

States that require notice to a state agency or attorney general include Alaska, California, Connecticut, Florida, Hawaii, Illinois, Indiana, Iowa, Maryland, Massachusetts, New York, North Carolina, South Carolina, Vermont, and Virginia. As noted above, attorney generals in California and New York have

[12] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches,* 105 Mich. L. Rev. 913, 962-63 (2007).

drawn on the information received due to these notifications in preparing reports on data breaches in their respective states.

Substantive Data Security. Beyond data breach notification, a handful of states create a substantive duty to take reasonable steps to safeguard data. Typically, these statutes provide open-ended, general standards, such as California's requirement to provide "reasonable security procedures and practices appropriate to the nature of the information." Cal. Pub. Util. Code § 8381 (2014). Other states with such laws include Oregon and Nevada. The Massachusetts Standards for the Protection of Personal Information is considered to be the strictest state security law. It extends to any business, no matter where located, that processes personal information of a resident of Massachusetts. 201 Mass. Code Regs. 17.03 (2014). The statute requires the development of a "readily accessible . . . comprehensive information security program" that is "appropriate to (a) the size, scope, and type of business . . . (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information."

Moreover, Massachusetts sets requirements beyond that of a security program. It calls for "the establishment and maintenance of a security system" that includes elements "to the extent technically feasible" including secure user authentication protocols, secure access control measures, and "encryption of all transmitted records and files containing personal information." An FAQ from the Office of Consumer Affairs and Business Regulation of Massachusetts warns that if it is not technically feasible to encrypt e-mail with personal information, the organization should "implement best practices by not sending unencrypted personal information in an email."[13]

Private Right of Action. Only a minority of the statutes provides a private right of action for individuals whose information has been breached. These states include Alaska, California, Maryland, Massachusetts, North Carolina, and Washington. In some states, the private right of action is found in the statute itself. In other states, the private right of action is located in the state's Unfair or Deceptive Trade Practices Act. State laws that do not have a private right of action generally assign their enforcement powers of the notification requirement to the attorney general.

Heightening Privacy Awareness Inside Corporations. Data breach notification laws have been found to play an important role in strengthening the "privacy function" in companies. According to Kenneth Bamberger and Deirdre Mulligan, the enactment of these statutes has been "an important driver of privacy in corporations."[14] In a series of interviews with leading privacy officials, Bamberger and Mulligan were told that corporate privacy officials were able to get

[13] Commonwealth of Massachusetts, Office of Consumer Affairs and Business Regulation, Frequently Asked Questions Regarding 201 CMR 17.00 (Nov. 3, 2009).

[14] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Ground* 71 (2015).

the attention of senior executives more easily because of these laws and found their roles enriched. In their summary, "Such laws . . . have served as a critical attention mechanism, transforming the effects of media coverage, and heightening consumer consciousness."[15]

C. CIVIL LIABILITY AND STANDING

In order to pursue a cause of action in federal court, plaintiffs must have standing. To establish standing, plaintiffs must show, among other things, that they have suffered an "injury in fact" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Friends of the Earth, Inc. v. Laidlaw Envtl. Sys. (TOC), Inc.*, 528 U.S. 167 (2000). If a plaintiff cannot establish standing, then a plaintiff's lawsuit cannot proceed forward in federal court.

REILLY V. CERIDIAN CORPORATION

664 F.3d 38 (3rd Cir. 2011)

ALDISERT, CJ. Kathy Reilly and Patricia Pluemacher, individually and on behalf of all others similarly situated, appeal from an order of the United States District Court for the District of New Jersey, which granted Ceridian Corporation's motion to dismiss for lack of standing, and alternatively, failure to state a claim. Appellants contend that (1) they have standing to bring their claims in federal court, and (2) they stated a claim that adequately alleged cognizable damage, injury, and ascertainable loss. We hold that Appellants lack standing and do not reach the merits of the substantive issue. We will therefore affirm.

Ceridian is a payroll processing firm with its principal place of business in Bloomington, Minnesota. To process its commercial business customers' payrolls, Ceridian collects information about its customers' employees. This information may include employees' names, addresses, social security numbers, dates of birth, and bank account information.

Reilly and Pluemacher were employees of the Brach Eichler law firm, a Ceridian customer, until September 2003. Ceridian entered into contracts with Appellants' employer and the employers of the proposed class members to provide payroll processing services.

On or about December 22, 2009, Ceridian suffered a security breach. An unknown hacker infiltrated Ceridian's Powerpay system and potentially gained access to personal and financial information belonging to Appellants and approximately 27,000 employees at 1,900 companies. It is not known whether the hacker read, copied, or understood the data.

Working with law enforcement and professional investigators, Ceridian determined what information the hacker may have accessed. On about January 29, 2010, Ceridian sent letters to the potential identity theft victims, informing them of the breach: "[S]ome of your personal information . . . may have been illegally

[15] Id. at 72.

accessed by an unauthorized hacker. . . . [T]he information accessed included your first name, last name, social security number and, in several cases, birth date and/or the bank account that is used for direct deposit." Ceridian arranged to provide the potentially affected individuals with one year of free credit monitoring and identity theft protection. Individuals had until April 30, 2010, to enroll in the free program, and Ceridian included instructions on how to do so within its letter.

Appellants' allegations of hypothetical, future injury do not establish standing under Article III. For the following reasons we will therefore affirm the District Court's dismissal.

Article III limits our jurisdiction to actual "cases or controversies." U.S. Const. art. III, § 2. One element of this "bedrock requirement" is that plaintiffs "must establish that they have standing to sue." *Raines v. Byrd,* 521 U.S. 811 (1997). It is the plaintiffs' burden, at the pleading stage, to establish standing. *See Lujan v. Defenders of Wildlife,* 504 U.S. 555 (1992).

We conclude that Appellants' allegations of hypothetical, future injury are insufficient to establish standing. Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.

The requirement that an injury be "certainly impending" is best illustrated by *City of Los Angeles v. Lyons,* 461 U.S. 95 (1983). There, the Court held that a plaintiff lacked standing to enjoin the Los Angeles Police Department from using a controversial chokehold technique on arrestees. Although the plaintiff had already once been subjected to this maneuver, the future harm he sought to enjoin depended on the police again arresting and choking him. Appellants in this case have yet to suffer any harm, and their alleged increased risk of future injury is nothing more than speculation. As such, the alleged injury is not "certainly impending." *Lujan.*

Our Court, too, has refused to confer standing when plaintiffs fail to allege an imminent injury-in-fact.

In this increasingly digitized world, a number of courts have had occasion to decide whether the "risk of future harm" posed by data security breaches confers standing on persons whose information *may* have been accessed. Most courts have held that such plaintiffs lack standing because the harm is too speculative. *See Amburgy v. Express Scripts, Inc.,* 671 F. Supp. 2d 1046 (E.D. Mo. 2009); *see also Key v. DSW Inc.,* 454 F. Supp. 2d 684 (S.D. Ohio 2006). We agree with the holdings in those cases. Here, no evidence suggests that the data has been—or will ever be—misused. The present test is actuality, not hypothetical speculations concerning the possibility of future injury. Appellants' allegations of an increased risk of identity theft resulting from a security breach are therefore insufficient to secure standing. . . .

[Regarding comparisons of data-security-breach situations to defective-medical-device, toxic-substance-exposure, or environmental-injury cases, the Third Circuit stated, "These analogies do not persuade us, because defective-

medical-device and toxic-substance-exposure cases confer standing based on two important factors not present in data breach cases."]

First, in those cases, an injury has undoubtedly occurred. In medical-device cases, a defective device has been implanted into the human body with a quantifiable risk of failure. Similarly, exposure to a toxic substance causes injury; cells are damaged and a disease mechanism has been introduced. Hence, the damage has been done; we just cannot yet quantify how it will manifest itself.

In data breach cases where no misuse is alleged, however, there has been no injury—indeed, no change in the status quo. Here, Appellants' credit card statements are exactly the same today as they would have been had Ceridian's database never been hacked. Moreover, there is no quantifiable risk of damage in the future. Any damages that may occur here are entirely speculative and dependent on the skill and intent of the hacker.

Second, standing in medical-device and toxic-tort cases hinges on human health concerns. . . . The deceased, after all, have little use for compensation. This case implicates none of these concerns. The hacker did not change or injure Appellants' bodies; any harm that may occur—if all of Appellants' stated fears are actually realized—may be redressed in due time through money damages after the harm occurs with no fear that litigants will be dead or disabled from the onset of the injury.

An analogy to environmental injury cases fails as well. [S]tanding is unique in the environmental context because monetary compensation may not adequately return plaintiffs to their original position. In a data breach case, however, there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely—*if* the hacked information is actually read, copied, understood, and misused to a plaintiff's detriment. To the contrary, unlike priceless "mountains majesty," the thing feared lost here is simple cash, which is easily and precisely compensable with a monetary award. We therefore decline to analogize this case to those cases in the medical device, toxic tort or environmental injury contexts.

Finally, we conclude that Appellants' alleged time and money expenditures to monitor their financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more "actual" injuries than the alleged "increased risk of injury" which forms the basis for Appellants' claims.

RESNICK V. AVMED

693 F.3d 1317 (11th Cir. 2012)

WILSON, CJ. Juana Curry and William Moore (collectively "Plaintiffs") appeal the district court's dismissal of their Second Amended Complaint ("Complaint") for failure to state a claim upon which relief may be granted. The district court held that among its other deficiencies, the Complaint failed to state a cognizable injury. We find that the complaint states a cognizable injury for the purposes of standing and as a necessary element of injury in Plaintiffs' Florida law claims. We also conclude that the Complaint sufficiently alleges the causation element of negligence, negligence *per se*, breach of contract, breach of implied contract,

breach of the implied covenant of good faith and fair dealing, and breach of fiduciary duty . . . . The Complaint similarly alleges facts sufficient to withstand a motion to dismiss on the restitution/unjust enrichment claim. However, the Complaint fails to allege entitlement to relief under Florida law for the claims of negligence *per se* and breach of the implied covenant of good faith and fair dealing. We therefore reverse in part, affirm in part, and remand the case to the district court for further proceedings.

AvMed, Inc. is a Florida corporation that delivers health care services through health plans and government-sponsored managed-care plans. AvMed has a corporate office in Gainesville, Florida, and in December 2009, two laptop computers were stolen from that office. Those laptops contained AvMed customers' sensitive information, which included protected health information, Social Security numbers, names, addresses, and phone numbers. AvMed did not take care to secure these laptops, so when they were stolen the information was readily accessible. The laptops were sold to an individual with a history of dealing in stolen property. The unencrypted laptops contained the sensitive information of approximately 1.2 million current and former AvMed members.

The laptops contained personal information of Juana Curry and William Moore. Plaintiffs are careful in guarding their sensitive information and had never been victims of identity theft before the laptops were stolen. Curry guards physical documents that contain her sensitive information and avoids storing or sharing her sensitive information digitally. Similarly, Moore guards physical documents that contain his sensitive information and is careful in the digital transmission of this information.

Notwithstanding their care, Plaintiffs have both become victims of identity theft. Curry's sensitive information was used by an unknown third party in October 2010—ten months after the laptop theft. Bank of America accounts were opened in Curry's name, credit cards were activated, and the cards were used to make unauthorized purchases. Curry's home address was also changed with the U.S. Postal Service. Moore's sensitive information was used by an unknown third party in February 2011 — fourteen months after the laptop theft. At that time, an account was opened in Moore's name with E*Trade Financial, and in April 2011, Moore was notified that the account had been overdrawn.

Prior to making an adjudication on the merits, we must assure ourselves that we have jurisdiction to hear the case before us. Litigants must show that their claim presents the court with a case or controversy under the Constitution and meets the "irreducible constitutional minimum of standing." *Lujan,* 504 U.S. at 560. To fulfill this requirement, a plaintiff must show that:

> (1) it has suffered an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167 (2000). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice" to establish standing. *Lujan.*

Whether a party claiming actual identity theft resulting from a data breach has standing to bring suit is an issue of first impression in this Circuit. Plaintiffs allege

that they have become victims of identity theft and have suffered monetary damages as a result. This constitutes an injury in fact under the law.[1]

We must next determine whether Plaintiffs' injury is fairly traceable to AvMed's actions. A showing that an injury is "fairly traceable" requires less than a showing of "proximate cause." *Focus on the Family v. Pinellas Suncoast Transit Auth.*, 344 F.3d 1263 (11th Cir. 2003). Even a showing that a plaintiff's injury is indirectly caused by a defendant's actions satisfies the fairly traceable requirement. Plaintiffs allege that AvMed failed to secure their information on company laptops, and that those laptops were subsequently stolen. Despite Plaintiffs' personal habits of securing their sensitive information, Plaintiffs became the victims of identity theft after the unencrypted laptops containing their sensitive information were stolen. For purposes of standing, these allegations are sufficient to "fairly trace" their injury to AvMed's failures.

Finally, Plaintiffs must show that a favorable resolution of the case in their favor could redress their alleged injuries. Plaintiffs allege a monetary injury and an award of compensatory damages would redress that injury. Plaintiffs have alleged sufficient facts to confer standing, and we now turn to the merits of their appeal. . . .

The complaint must contain enough facts to make a claim for relief plausible on its face; a party must plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged."

. . . Plaintiffs brought seven counts against AvMed, all under Florida law. Of the seven causes of action alleged, Florida law requires a plaintiff to show that the defendant's challenged action *caused* the plaintiff's harm in six of them: negligence, negligence *per se,* breach of fiduciary duty, breach of contract, breach of contract implied in fact, and breach of the implied covenant of good faith and fair dealing. A negligence claim requires a plaintiff to show that (1) defendants owe plaintiffs a duty, (2) defendants breached the duty, (3) defendants' breach injured plaintiffs, and "(4) [plaintiffs'] damage [was] *caused by* the injury to the plaintiff as a result of the defendant's breach of duty." Similarly, under Florida law, an action for negligence *per* se requires a plaintiff to show "violation of a statute which establishes a duty to take precautions to protect a particular class of persons from a particularly injury or type of injury." As part of this showing, plaintiffs must establish "that the violation of the statute *was the proximate cause* of [their] injury." The elements of a cause of action for breach of fiduciary duty in Florida include "damages *flowing from* the breach."

The contract claims also require a showing of causation. In Florida, a breach of contract claim requires a party to show that *damages resulted from* the breach. Florida courts use breach of contract analysis to evaluate claims of breach of contract implied in fact and breach of the covenant of good faith and fair dealing.

We now consider the well-pleaded factual allegations relating to causation.... The complaint alleges that, prior to the data breach, neither Curry nor Moore had ever had their identities stolen or their sensitive information "compromised in any way." It further alleges that "Curry took substantial precautions to protect herself from identity theft," including not transmitting sensitive information over the Internet or any unsecured source; not storing her sensitive information on a computer or media device; storing sensitive information in a "safe and secure physical location;" and destroying "documents she receives in the mail that may contain any of her sensitive information, or that contain any information that could otherwise be used to steal her identity, such as credit card offers." Similarly, Moore alleges in the complaint that he "took substantial precautions to protect himself from identity theft," including not transmitting unencrypted sensitive information over the internet or any other source, storing documents containing sensitive information "in a safe and secure physical location and destroy[ing] any documents he receives in the mail" that include either sensitive information or information that "could otherwise be used to steal his identity." Plaintiffs became victims of identity theft for the first time in their lives ten and fourteen months after the laptops containing their sensitive information were stolen. Curry's sensitive information was used to open a Bank of America account and change her address with the United States Post Office, and Moore's sensitive information was used to open an E*Trade Financial account in his name.

Our task is to determine whether the pleadings contain "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " A claim is facially plausible when the court can draw "the reasonable inference that the defendant is liable for the misconduct alleged" from the pled facts. Taken as true, these factual allegations are consistent with Plaintiffs' conclusion that AvMed's failure to secure Plaintiffs' information caused them to become victims of identity theft. After thorough consideration, we conclude that the allegations are sufficient to cross the line from merely possible to plausible.

Generally, to prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence. . . . Here, Plaintiffs allege a nexus between the two events that includes more than a coincidence of time and sequence: they allege that the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs' identity. Plaintiffs explicitly make this connection when they allege that Curry's identity was stolen by changing her address and that Moore's identity was stolen by opening an E*Trade Financial account in his name because in both of those allegations, Plaintiffs state that the identity thief used Plaintiffs' sensitive information. We understand Plaintiffs to make a similar allegation regarding the bank accounts opened in Curry's name even though they do not plead precisely that Curry's sensitive information was used to open the Bank of America account. The Complaint states that Curry's sensitive information was on the unencrypted stolen laptop, that her identity was stolen, and that the *stolen identity* was used to open unauthorized accounts. Considering the Complaint as a whole and applying common sense to our understanding of this allegation, we find that Plaintiffs allege that the same sensitive information that was stored on the stolen laptops was used to open the Bank of America account. Thus, Plaintiffs' allegations that the data breach caused their identities to be stolen move from the realm of the possible into the plausible. Had Plaintiffs alleged fewer facts, we doubt whether the Complaint could have survived a motion to dismiss. However, Plaintiffs have sufficiently alleged a nexus between the data theft and the identity theft and therefore meet the federal pleading standards. Because their contention that the data breach caused the identity theft is plausible under the facts pled, Plaintiffs meet the pleading standards for their allegations on the counts of negligence, negligence *per se,* breach of fiduciary duty, breach of contract, breach

of implied contract, and breach of the implied covenant of good faith and fair dealing. . . .

To establish a cause of action for unjust enrichment/restitution, a Plaintiff must show that "1) the plaintiff has conferred a benefit on the defendant; 2) the defendant has knowledge of the benefit; 3) the defendant has accepted or retained the benefit conferred; and 4) the circumstances are such that it would be inequitable for the defendant to retain the benefit without paying fair value for it." *Della Ratta v. Della Ratta*, 927 So. 2d 1055, 1059 (Fla. Dist. Ct. App. 2006).

Plaintiffs allege that they conferred a monetary benefit on AvMed in the form of monthly premiums, that AvMed "appreciates or has knowledge of such benefit," that AvMed uses the premiums to "pay for the administrative costs of data management and security," and that AvMed "should not be permitted to retain the money belonging to Plaintiffs ... because [AvMed] failed to implement the data management and security measures that are mandated by industry standards." Plaintiffs also allege that AvMed either failed to implement or inadequately implemented policies to secure sensitive information, as can be seen from the data breach. Accepting these allegations as true, we find that Plaintiffs alleged sufficient facts to allow this claim to survive a motion to dismiss. . . .

AvMed argues that we can affirm the district court because the Complaint fails to allege an entitlement to relief under Florida law on each count. On review, we find that two of the pled causes of action do not allow Plaintiffs to recover under Florida law. We address only the two claims that fail: negligence *per se,* and breach of the covenant of good faith and fair dealing. . . .

[The Eleventh Circuit found that the negligence *per se* failed because the statutory section that the plaintiffs argued was contained in a chapter regulating the licensure, development, establishment, and minimum standard enforcement of hospitals, ambulatory surgical centers, and mobile surgical facilities. Fla. Stat. § 395.001. It stated: "Because AvMed is an integrated managed-care organization and not a hospital, ambulatory surgical center, or mobile surgical facility, AvMed is not subject to this statute."

The Eleventh Circuit also found that there was no violation of the implied covenant of good faith and fair dealing under Florida law by Avmed. Florida requires a "conscious act" to frustrate the common purpose of a contract and the Plaintiffs failed to allege "AvMed's shortcomings were conscious acts to frustrate the common purpose of the agreement."]

In this digital age, our personal information is increasingly becoming susceptible to attack. People with nefarious interests are taking advantage of the plethora of opportunities to gain access to our private information and use it in ways that cause real harm. Even though the perpetrators of these crimes often remain unidentified and the victims are left to clean up the damage caused by these identity thieves, cases brought by these victims are subject to the same pleading standards as are plaintiffs in all civil suits. Here, Plaintiffs have pled a cognizable injury and have pled sufficient facts to allow for a plausible inference that AvMed's failures in securing their data resulted in their identities being stolen. They have shown a sufficient nexus between the data breach and the identity theft beyond allegations of time and sequence.

PRYOR, CJ., dissenting. I agree with the majority opinion that Curry and Moore have standing to sue, but Curry and Moore's complaint should be dismissed for failure to state a claim. Their complaint fails to allege a plausible basis for finding that AvMed caused them to suffer identity theft, and their claim of unjust enrichment fails as a matter of law. . . .

The parties do not dispute that laptops containing the sensitive information of Curry and Moore was stolen from AvMed, but Curry and Moore's second amended complaint fails to plead enough facts to allow a factfinder to draw a reasonable inference that the sensitive information identity thieves used to open the fraudulent accounts in the plaintiffs' names was obtained from AvMed. In an attempt to bridge this gap, Curry and Moore allege that they have both been *very* careful to protect their sensitive information. But the manner in which Curry and Moore care for the sensitive information they receive from third parties tells us nothing about how the third parties care for that sensitive information before or after they send it to Curry and Moore.

Regarding the cause of the identity theft that Curry and Moore suffered it is conceivable that the unknown identity thieves used the sensitive information stolen from AvMed to open the fraudulent accounts, but it is equally conceivable, in the light of the facts alleged in the complaint, that the unknown identity thieves obtained the information from third parties. Curry and Moore do not allege any facts that make it plausible that the unknown identity thieves who opened the fraudulent accounts obtained the sensitive information necessary to do so from AvMed. . . .

The complaint also fails to state a claim of unjust enrichment under Florida law. "Florida courts have held that a plaintiff cannot pursue a quasi-contract claim for unjust enrichment if an express contract exists concerning the same subject matter." The parties do not dispute that they entered into an enforceable contract; they dispute whether the contract has been breached. In that circumstance, a claim of unjust enrichment cannot be maintained.

I respectfully dissent.

NOTES & QUESTIONS

1. ***Harm? No Harm?*** The stakes in data security breach litigation are high. Plaintiffs want companies to guard their information more carefully and are concerned about identity theft. Companies face considerable financial exposure. Consider that after the Eleventh Circuit allowed the lawsuit in *Resnick* to continue, AvMed negotiated a $3 million settlement quickly with the attorneys for the plaintiffs. That is a high cost for leaving two laptops unsecured in a corporate office.

   This high stakes litigation is also accompanied by legal uncertainty regarding the nature of the harm to plaintiffs and whether standing is present. *Reilly* and *Resnick* evaluated a different range of claims and reached sometimes contrary results. Analogies were attempted with toxic torts, defective medical devices, and environmental injury. Do you find any of these areas closer or farther from the concerns in data security? In *Resnick*, the plaintiffs were actual

victims of identity theft occurring after the theft of the AvMed laptops. Why does that fact make a difference for the Eleventh Circuit?

2. ***Tort Negligence for Data Security Breaches.*** In tort law, under a general negligence theory, litigants might sue a company after a data security incident and seek to collect damages. In contrast to *Resnick*, however, many class action lawsuits following data breaches have been notably unsuccessful. Among other problems, claimants are facing trouble convincing courts that the data processing entities owe a duty to the individuals whose data are leaked, or that damages can be inferred from the simple fact of a data breach. For example, a South Carolina court declared in 2003 that "[t]he relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them." *Huggins v. Citibank*, 585 S.E.2d 275 (S.C. 2003).
3. ***Proving Injury from Data Security Breaches: Three Theories of Harm.*** Suppose a person has been notified that her personal information has been improperly accessed, but she has not yet suffered from identity theft. Should she be entitled to any form of compensation? Has she suffered an injury? One might argue that being made more vulnerable to future harm has made her worse off than before. The individual might live with greater unease knowing that she is less secure. On the other hand, no identity theft has occurred, and it may never occur. How should the law address this situation? Recognize a harm? If so, how should damages be assessed?

   For data security breaches, plaintiffs have generally advanced one or more of the following theories of harm:

   (1) *Emotional Distress.* The exposure of their data has caused them emotional distress.
   (2) *Increased Risk of Future Harm.* The exposure of their data has subjected them to an increased risk of harm from identity theft, fraud, or other injury.
   (3) *Expenditures to Reduce Risk of Future Harm.* The exposure of their data has resulted in their having to expend time and money to prevent future fraud, such as signing up for credit monitoring, contacting credit reporting agencies and placing fraud alerts on their accounts, and so on.

Courts are divided on whether to recognize harm on these theories, but the majority of courts have dismissed all of these theories. According to Daniel Solove and Danielle Keats Citron, many courts take a "visceral and vested" approach to harm: "Courts insist that data harms be visceral—easy to see, measure, and quantify. They require harms to be vested—already materialized in the here and now. Plaintiffs must experience physical, monetary, or property damage or, at least, the damage must be imminent."

Solove and Citron observe:

> This cramped understanding of harm harkens back to early conceptions of the common law. Nineteenth-century tort claims required proof of physical injury or property loss. Financial losses could be recovered in tort actions if defendants owed plaintiffs a special duty of care. Along these lines, courts have recognized claims for privacy violations only where redress is sought for tangible financial losses. Courts have found a sufficient injury in data breach cases where the exposure of personal data has led to identity theft. But without proof of physical harm or financial loss, courts rarely recognize harm.
>
> Requiring harm to be visceral and vested has severely restricted the recognition of data harms, which rarely have these qualities. Data breach harms are not easy to see, at least not in any physical way. They are not tangible like broken limbs and destroyed property. Instead, the harm is intangible. Data breaches increase a person's risk of identity theft or fraud and cause emotional distress as a result of that risk.[16]

4. ***Emotional Distress.*** The majority of courts are reluctant to recognize emotional distress as a harm stemming from a data breach. Solove and Citron explain why:

   > A concern with recognizing emotional distress in data breach cases is that psychic distress can be readily manufactured. Arguments against the recognition of anxiety focus on the fact that claims of anxiety are easy to make and difficult to dispute. Plaintiffs will quickly learn to make poignant statements about their anguish, with statements exaggerating their distress. Defendants may have difficulty disproving plaintiffs' accounts of their own subjective mental states.[17]

   However, Solove and Citron go on to note that in many other areas of law, courts readily move past these concerns to recognize pure emotional distress as a basis of harm:

   > [T]he law has evolved to recognize emotional distress disconnected from physical or financial injury. In certain privacy cases, courts recognize pure emotional distress without hesitation, most likely, we posit, because courts recognize that most people would feel emotional distress in these situations. In essence, an unstated objective test to emotional distress seems to exist in privacy tort cases.

5. ***Increased Risk of Future Harm.*** In *Resnick*, the plaintiffs suffered identity fraud several months after the breach and the Eleventh Circuit concluded that their allegations were sufficient to "fairly trace" their injury to AvMed's information security failures. Would the court have reached the same conclusion if hackers had accessed data but there were no incidences of identity theft or fraud?

   In *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), the court concluded that increased vulnerability to identity theft could give rise to standing based upon the theft of a laptop containing unencrypted personal data:

---

[16] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 Tex. L. Rev. — (forthcoming 2017).

[17] *Id.*

> Here, Plaintiffs–Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data. Were Plaintiffs–Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible. On these facts, however, Plaintiffs–Appellants have sufficiently alleged an injury-in-fact for purposes of Article III standing.

6. ***Expenditures to Reduce Risk of Future Harm.*** Why do most courts conclude that expenditures to reduce risks of future harm created by another are not recoverable? Suppose a company leaks a toxic chemical, causing a person to have an increased risk of cancer. The person sees a doctor and gets a prescription for a drug that will reduce the likelihood that the chemical will cause cancer. Would the expenses of seeing the doctor and purchasing the drug be recoverable? Is this hypothetical analogous to a data security breach?
7. ***The Impact of* Clapper**. A 2013 Supreme Court case involving a constitutional challenge to national security surveillance had become a key and contested precedent for the issue of standing in data breach cases. In *Clapper v. Amnesty International USA*, 133 S. Ct. (2013), a group of attorneys, journalists, and others contended that government surveillance under the Foreign Intelligence Surveillance Act (FISA) violated their constitutional rights. They could not establish that they were definitely under surveillance, but they had a legitimate reason to suspect that they were under surveillance because they represented or spoke to individuals who the government viewed as suspicious.

   The Supreme Court held that the plaintiffs could not establish standing. The Court reasoned that "it is speculative whether the Government will imminently target communications to which respondents are parties."

   The plaintiffs also contended that they were injured because they had to take measures to avoid the risk that they were under surveillance. "Respondents claim, for instance, that the threat of surveillance sometimes compels them to avoid certain e-mail and phone conversations, to 'tal[k] in generalities rather than specifics,' or to travel so that they can have in-person conversations." The Court rejected these costs as a basis for injury because "parties cannot manufacture standing by incurring costs in anticipation of non-imminent harm."

   Many courts have used *Clapper* to deny standing to plaintiffs in data breach cases when plaintiffs claim injury due to an increased risk of future harm or expenditures to reduce the risk of future harm. Other courts have held that *Clapper* does not foreclose finding harm on these theories. Consider the cases that follow.

REMIJAS V. NEIMAN MARCUS CORP.

794 F.3d 688 (7th Cir. 2015)

WOOD, J. Sometime in 2013, hackers attacked Neiman Marcus, a luxury department store, and stole the credit card numbers of its customers. In December 2013, the company learned that some of its customers had found fraudulent charges

on their cards. On January 10, 2014, it announced to the public that the cyberattack had occurred and that between July 16, 2013, and October 30, 2013, approximately 350,000 cards had been exposed to the hackers' malware. In the wake of those disclosures, several customers brought this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), seeking various forms of relief. The district court stopped the suit in its tracks, however, ruling that both the individual plaintiffs and the class lacked standing under Article III of the Constitution. This resulted in a dismissal of the complaint without prejudice. We conclude that the district court erred. The plaintiffs satisfy Article III's requirements based on at least some of the injuries they have identified. We thus reverse and remand for further proceedings.

. . .

The plaintiffs . . . allege that they have standing based on two imminent injuries: an increased risk of future fraudulent charges and greater susceptibility to identity theft. We address the two alleged imminent injuries first and then the four asserted actual injuries.

Allegations of future harm can establish Article III standing if that harm is "certainly impending," but "allegations of possible future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138 (2013). Here, the complaint alleges that everyone's personal data has already been stolen; it alleges that the 9,200 who already have incurred fraudulent charges have experienced harm. Those victims have suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges. The complaint also alleges a concrete risk of harm for the rest. The question is whether these allegations satisfy *Clapper*'s requirement that injury either already have occurred or be "certainly impending."

As for the 9,200 (including Frank and Farnoush), the plaintiffs concede that they were later reimbursed and that the evidence does not yet indicate that their identities (as opposed to the data) have been stolen. But as we already have noted, there are identifiable costs associated with the process of sorting things out. Neiman Marcus challenges the standing of these class members, but we see no merit in that point. What about the class members who contend that un-reimbursed fraudulent charges and identity theft may happen in the future, and that these injuries are likely enough that immediate preventive measures are necessary? Neiman Marcus contends that this is too speculative to serve as injury-in-fact. It argues that all of the plaintiffs would be reimbursed for fraudulent charges because (it asserts) that is the common practice of major credit card companies. The plaintiffs disagree with the latter proposition; they contend that they, like all consumers subject to fraudulent charges, must spend time and money replacing cards and monitoring their credit score, and that full reimbursement is not guaranteed. (It would not be enough to review one's credit card statements carefully every month, because the thieves might—and often do—acquire new credit cards unbeknownst to the victim.) This reveals a material factual dispute on such matters as the class members' experiences and both the content of, and the universality of, bank reimbursement policies.

Clapper does not, as the district court thought, foreclose any use whatsoever of future injuries to support Article III standing. In *Clapper*, the Supreme Court decided that human rights organizations did not have standing to challenge the

Foreign Intelligence Surveillance Act (FISA) because they could not show that their communications with suspected terrorists were intercepted by the government. The plaintiffs only suspected that such interceptions might have occurred. This, the Court held, was too speculative to support standing. In so ruling, however, it did not jettison the "substantial risk" standard. To the contrary, it stated that "[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." . . . .

The plaintiffs allege that the hackers deliberately targeted Neiman Marcus in order to obtain their credit-card information. Whereas in *Clapper*, "there was no evidence that any of respondents' communications either had been or would be monitored," in our case there is "no need to speculate as to whether [the Neiman Marcus customers'] information has been stolen and what information was taken." . . . . [T]he Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an "objectively reasonable likelihood" that such an injury will occur. . . .

At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities. The plaintiffs are also careful to say that only 9,200 cards have experienced fraudulent charges so far; the complaint asserts that fraudulent charges and identity theft can occur long after a data breach. It cites a Government Accountability Office Report that finds that "stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years." U.S. Gov't Accountability Office, GAO-07-737, *Report to Congressional Requesters: Personal Information* 29 (2007). . . .

In addition to the alleged future injuries, the plaintiffs assert that they have already lost time and money protecting themselves against future identity theft and fraudulent charges. Mitigation expenses do not qualify as actual injuries where the harm is not imminent. *Clapper*, 133 S.Ct. at 1152 (concluding that "costs that they have incurred to avoid [injury]" are insufficient to confer standing). Plaintiffs "cannot manufacture standing by incurring costs in anticipation of non-imminent harm." *Id.* at 1155. . . .

Once again, however, it is important not to overread *Clapper*. *Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs. In our case, Neiman Marcus does not contest the fact that the initial breach took place. An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring. It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded. These credit-monitoring services come at a price that is more than de minimis. For instance, Experian offers credit monitoring for $4.95 a month for the first month, and then $19.95 per month thereafter. That easily qualifies as a concrete injury. . . .

BECK V. MCDONALD

949 F.3d 262 (4th Cir. 2017)

DIAZ, J. The Plaintiffs in these consolidated appeals are veterans who received medical treatment and health care at the William Jennings Bryan Dorn Veterans Affairs Medical Center ("Dorn VAMC") in Columbia, South Carolina. After two data breaches at the Center compromised their personal information, the Plaintiffs brought separate actions against the Secretary of Veterans Affairs and Dorn VAMC officials ("Defendants"), alleging violations of the Privacy Act of 1974, 5 U.S.C. § 552a *et seq.* and the Administrative Procedure Act ("APA"), 5 U.S.C. § 701 *et seq.*

In both cases, the Plaintiffs sought to establish Article III standing based on the harm from the increased risk of future identity theft and the cost of measures to protect against it. The district court dismissed the actions for lack of subject-matter jurisdiction, holding that the Plaintiffs failed to establish a non-speculative, imminent injury-in-fact for purposes of Article III standing. We agree with the district court and therefore affirm.

The Beck case arises from a report that on February 11, 2013, a laptop connected to a pulmonary function testing device with a Velcro strip was misplaced or stolen from Dorn VAMC's Respiratory Therapy department. The laptop contains unencrypted personal information of approximately 7,400 patients, including names, birth dates, the last four digits of social security numbers, and physical descriptors (age, race, gender, height, and weight).

An internal investigation determined that the laptop was likely stolen and that Dorn VAMC failed to follow the policies and procedures for utilizing a non-encrypted laptop to store patient information. Dorn VAMC officials used medical appointment records to notify every patient tested using the missing laptop and offered one year of free credit monitoring. To date, the laptop has not been recovered.

Richard Beck and Lakreshia Jeffery (the "Beck plaintiffs") filed suit on behalf of a putative class of the approximately 7,400 patients whose information was stored on the missing laptop. Relevant to this appeal, the Beck plaintiffs sought declaratory relief and monetary damages under the Privacy Act, alleging that the "Defendants' failures" and "violations" of the Privacy Act "caused Plaintiffs . . . embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse of their Personal Information." J. They further allege that the "threat of identity theft" required them to frequently monitor their "credit reports, bank statements, health insurance reports, and other similar information, purchas[e] credit watch services, and [shift] financial accounts." . . . .

The district court granted the Defendants' motion to dismiss, holding, pursuant to *Clapper v. Amnesty International USA*, 133 S.Ct. 1138 (2013), that the Beck plaintiffs lacked standing under the Privacy Act because they had "not submitted

evidence sufficient to create a genuine issue of material fact as to whether they face a 'certainly impending' risk of identity theft." . . . .

The Watson case arises from Dorn VAMC's July 2014 discovery that four boxes of pathology reports headed for long-term storage had been misplaced or stolen. The reports contain identifying information of over 2,000 patients, including names, social security numbers, and medical diagnoses. Dorn VAMC officials alerted those affected and, as they did following the laptop's disappearance, offered each of them one year of free credit monitoring. The boxes have not been recovered.

While the Beck litigation was pending, Beverly Watson brought a putative class-action lawsuit on behalf of the over 2,000 individuals whose pathology reports had gone missing. Watson sought money damages and declaratory and injunctive relief, alleging the same harm as did the Beck plaintiffs. The Defendants moved to dismiss the complaint for lack of subject-matter jurisdiction and for failure to state a claim.

The district court granted the Defendants' motion to dismiss for lack of subject-matter jurisdiction, relying on *Clapper* to hold that Watson lacked Article III standing under the Privacy Act because she "ha[d] not alleged that there ha[d] been any actual or attempted misuse of her personal information," thus rendering her allegation that her information "will eventually be misused as a result of the disappearance of the boxes . . . speculative." . . . .

We focus our inquiry on the first element of Article III standing: injury-in-fact. "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016). . . .

Clapper's discussion of when a threatened injury constitutes an Article III injury-in-fact is controlling here. Before explaining why, we address the Plaintiffs' contention that the district court misread *Clapper* to require a new, heightened burden for proving an Article III injury-in-fact. To the contrary, *Clapper*'s iteration of the well-established tenet that a threatened injury must be "certainly impending" to constitute an injury-in-fact is hardly novel.

We also reject the Plaintiffs' claim that "emotional upset" and "fear [of] identity theft and financial fraud" resulting from the data breaches are "adverse effects" sufficient to confer Article III standing. . . .

Our sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft. The Sixth, Seventh, and Ninth Circuits have all recognized, at the pleading stage, that plaintiffs can establish an injury-in-fact based on this threatened injury. *See Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed.Appx. 384 (6th Cir. 2016) (plaintiff-customers' increased risk of future identity theft theory established injury-in-fact after hackers breached Nationwide Mutual Insurance Company's computer network and stole their sensitive personal information, because "[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals"); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015) (plaintiff-customers' increased risk of future fraudulent charges and identity theft theory established "certainly impending" injury-in-fact and "substantial risk of harm" after hackers attacked Neiman Marcus with malware to steal credit card numbers, because "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) (plaintiff-employees' increased risk of future identity theft theory a "credible threat of harm" for Article III purposes after theft of a laptop containing the unencrypted names, addresses, and social security numbers of 97,000 Starbucks employees). . . .

By contrast, the First and Third Circuits have rejected such allegations. *See Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012) (brokerage account-holder's increased risk of unauthorized access and identity theft theory insufficient to constitute "actual or impending injury" after defendant failed to properly maintain an electronic platform containing her account information, because plaintiff failed to "identify any incident in which her data has ever been accessed by an unauthorized person"); *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (plaintiff-employees' increased risk of identity theft theory too hypothetical and speculative to establish "certainly impending" injury-in-fact after unknown hacker penetrated payroll system firewall, because it was "not known whether the hacker read, copied, or understood" the system's information and no evidence suggested past or future misuse of employee data or that the "intrusion was intentional or malicious").

The Plaintiffs say that our sister circuits' decisions in *Krottner, Pisciotta*, and *Remijas* support their allegations of standing based on threatened injury of future identity theft. To the contrary, these cases demonstrate why the Plaintiffs' theory is too speculative to constitute an injury-in-fact.

Underlying the cases are common allegations that sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent. In *Galaria, Remijas*, and *Pisciotta*, for example, the data thief intentionally targeted the personal information compromised in the data breaches. . . . And, in *Remijas* and *Krottner*, at least one named plaintiff alleged misuse or access of that personal information by the thief.

Here, the Plaintiffs make no such claims. This in turn renders their contention of an enhanced risk of future identity theft too speculative. On this point, the data breaches in Beck and Watson occurred in February 2013 and July 2014, respectively. Yet, even after extensive discovery, the Beck plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information. Watson's complaint suffers from the same deficiency with regard to the four missing boxes of pathology reports. Moreover, "as the breaches fade further into the past," the Plaintiffs' threatened injuries become more and more speculative.

The Plaintiffs counter that there is "no need to speculate" here because they have alleged—and in the Beck case the VA's investigation concluded—that the laptop and pathology reports had been stolen. We of course accept this allegation as true. But the mere theft of these items, without more, cannot confer Article III standing.

Indeed, for the Plaintiffs to suffer the harm of identity theft that they fear, we must engage with the same "attenuated chain of possibilities" rejected by the Court in *Clapper*. In both cases, we must assume that the thief targeted the stolen items for the personal information they contained. And in both cases, the thieves must

then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities. This "attenuated chain" cannot confer standing. . . .

Nonetheless, our inquiry on standing is not at an end, for we may also find standing based on a "substantial risk" that the harm will occur, which in turn may prompt a party to reasonably incur costs to mitigate or avoid that harm. But here too the Plaintiffs fall short of their burden.

The Plaintiffs allege that: (1) 33% of health-related data breaches result in identity theft; (2) the Defendants expend millions of dollars trying to avoid and mitigate those risks; and (3) by offering the Plaintiffs free credit monitoring, the VA effectively conceded that the theft of the laptop and pathology reports constituted a "reasonable risk of harm to those victimized" by the data breaches.

These allegations are insufficient to establish a "substantial risk" of harm. Even if we credit the Plaintiffs' allegation that 33% of those affected by Dorn VAMC data breaches will become victims of identity theft, it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a "substantial risk" of harm. *E.g., Khan v. Children's Nat'l Health Sys.*, 188 F.Supp.3d 524 (D. Md. 2016) ("general allegations . . . that data breach victims are 9.5 times more likely to suffer identity theft and that 19 percent of data breach victims become victims of identity theft" insufficient to establish "substantial risk" of harm); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F.Supp.3d 14, 26 (D.D.C. 2014) (no "substantial risk" of harm where "[b]y Plaintiff's own calculations, then, injury is likely not impending for over 80% of victims").

The Plaintiffs' other allegations fare no better. Contrary to some of our sister circuits, we decline to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals. To adopt such a presumption would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit. . . .

Next, we turn to the Plaintiffs' allegation that they have suffered an injury-in-fact because they have incurred or will in the future incur the cost of measures to guard against identity theft, including the costs of credit monitoring services. All Plaintiffs allege that they wish to enroll in, are enrolled in, or have purchased credit monitoring services. They also say that, as a consequence of the breaches, they have incurred the burden of monitoring their financial and credit information. Even accepting these allegations as true, they do not constitute an injury-in-fact.

As was the case in *Clapper*, the Plaintiffs here seek "to bring this action based on costs they incurred in response to a speculative threat," i.e. their fear of future identity theft based on the breaches at Dorn VAMC. But this allegation is merely "a repackaged version of [Plaintiffs'] first failed theory of standing." Simply put, these self-imposed harms cannot confer standing. . . ..

We acknowledge that the named plaintiffs have been victimized by "at least two admitted VA data breaches," and that Ms. Watson's information was compromised in both the 2013 laptop theft and the 2014 pathology reports theft. . . . The most that can be reasonably inferred from the Plaintiffs' allegations regarding the likelihood of another data breach at Dorn VAMC is that the Plaintiffs could be victimized by a future data breach. That alone is not enough.

NOTES & QUESTIONS

1. ***A Circuit Split?*** There appears to be a circuit split over the impact of *Clapper* on data breach cases. Are *Remijas* and *Beck* inconsistent? *Beck* distinguishes *Remijas* because in *Remijas*, there was evidence that the "data thief intentionally targeted the personal information compromised in the data breaches" and "at least one named plaintiff alleged misuse or access of that personal information by the thief." Would the *Remijas* court have reached the same conclusion as the *Beck* court had it faced the same facts as in *Beck*?

   Suppose hackers cause the data breach rather than the data simply being lost or stolen. Also suppose that there have been no incidents of identity theft or fraud. Under the reasoning of *Remijas,* would plaintiffs have standing? How about under the reasoning of *Beck*?

   Courts are divided under these circumstances. For example, in *Storm v. Paytime, Inc.*, 90 F.Supp.3d 359 (M.D.Pa. 2015), the court denied standing to plaintiffs whose data was improperly accessed by a hacker:

   > Plaintiffs do not allege that they have actually suffered any form of identity theft as a result of the data breach—to wit, they have not alleged that their bank accounts have been accessed, that credit cards have been opened in their names, or that unknown third parties have used their Social Security numbers to impersonate them and gain access to their accounts. See Reilly, 664 F.3d at 45. In sum, their credit information and bank accounts look the same today as they did prior to Paytime's data breach in April 2014.

   In *Peters v. St. Joseph Servs. Corp.*, 74 F.Supp.3d 847 (S.D.Tex.2015), a health care provider was hacked and data about 405,000 people was compromised. The court held:

   > Peters' alleged future injuries are speculative—even hypothetical—but certainly not imminent. . . . For example, Peters might be able to demonstrate harm if third parties become aware of her exposed information and reveal their interest in it; if they form an intent to misuse her information; and if they take steps to acquire and actually use her information to her detriment. The misuse of her information could take any number of forms, at any point in time. The risk of future harm is, no doubt, indefinite. It may even be impossible to determine whether the misused information was obtained from exposure caused by the Data Breach or from some other source. . . .
   >
   > Under *Clapper*, Peters must at least plausibly establish a "certainly impending" or "substantial" risk that she will be victimized. The allegation that risk has been increased does not transform that assertion into a cognizable injury. In fact, as one district court has observed, "*Clapper* seems rather plainly to reject the premise . . . that any marginal increase in risk is sufficient to confer standing." *Strautins v. Trustwave Holdings, Inc.,* 27 F.Supp.3d 871, 878 (N.D.Ill.2014). . .
   >
   > The Court recognizes that before Clapper, a split existed among the Third, Seventh and Ninth circuit courts over whether the increased risk of harm stemming from a data security breach constitutes imminent injury under Article III. The Seventh and Ninth Circuits held that such a risk was sufficient to confer standing. *Krottner*, 628 F.3d 1139; *Pisciotta*, 499 F.3d 629. The Third Circuit held that the risk fails the constitutional test. *Reilly*, 664 F.3d at 42–45.

Arguably, *Clapper* has resolved the circuit split. Its holding compels the conclusion that Peters lacks standing to bring her federal claims to the extent they are premised on the heightened risk of future identity theft/fraud.

Does *Clapper* resolve the circuit split? Would the courts in *Remijas* and *Beck* agree?

In contrast to *Storm* and *Peters,* consider *In re Adobe Sys., Inc. Privacy Litigation*, 66 F.Supp.3d 1197 (N.D.Cal.2014), where the court concluded that plaintiffs had standing when a hacker gathered their personal data from Adobe's servers for several weeks:

> Unlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both "highly attenuated" and "highly speculative," the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real. Plaintiffs allege that the hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates. Plaintiffs' personal information was among the information taken during the breach. Thus, in contrast to *Clapper*, where there was no evidence that any of respondents' communications either had been or would be monitored under Section 702, here there is no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken.
>
> Neither is there any need to speculate as to whether the hackers intend to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so. Not only did the hackers deliberately target Adobe's servers, but Plaintiffs allege that the hackers used Adobe's own systems to decrypt customer credit card numbers. Some of the stolen data has already surfaced on the Internet, and other hackers have allegedly misused it to discover vulnerabilities in Adobe's products. Given this, the danger that Plaintiffs' stolen data will be subject to misuse can plausibly be described as "certainly impending." Indeed, the threatened injury here could be more imminent only if Plaintiffs could allege that their stolen personal information had already been misused. However, to require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be "literally certain" in order to constitute injury-in-fact.

2. ***The Nature of Data Security Harms.*** Consider Solove and Citron:

> To the individuals whose personal data is leaked into the hands of thieves, the risk of harm is continuing. Hackers may not use the personal data in the near term to steal bank accounts and take out loans. Instead, they may wait until an illness befalls a family member and then use personal data to generate medical bills in a victim's name. They may use the personal data a year later but only use some individuals' personal information for fraud. Although not all of the personal data will be used for criminal ends, some will. In the meanwhile, the individuals worry that their information will be misused and expend time and resources to protect themselves from this possibility.
>
> Long-term risk is not a harmless wrong unlike the risky driver who does not hurt anyone. It is not negligence "in the air," which the law has long understood as unworthy of a legal response.[18] There is an injury; it is not a regrettable close call like the reckless driver who hits no one. When an entity inadequately secures personal data and thieves steal it, the entity's unreasonable actions impact a sizeable number of users, often in the millions, and the excess risk of fraud is certain to take its toll on a number of those users. Over time, the risk will materialize for a percentage of those users. Although the eventual victims cannot be immediately identified, the entity cannot deny the reality of the loss it has inflicted.[19]

Ryan Calo has proposed a theory for how privacy harms should be understood:

> [T]he vast majority of privacy harms fall into just two categories — one subjective, the other objective. The subjective category of privacy harm is the perception of unwanted observation. This category describes unwelcome mental states — anxiety, for instance, or embarrassment — that accompany the belief that one is or will be watched or monitored. . . .
>
> The objective category of privacy harm is the unanticipated or coerced use of information concerning a person against that person. These are negative, external actions justified by reference to personal information. Examples include the unanticipated sale of a user's contact information that results in spam and the leaking of classified information that exposes an undercover intelligence agent.

How does Calo's theory apply to data security breaches? Consider his analysis:

> As an initial matter, data breaches register as subjective privacy harms. When a consumer receives a notice in the mail telling her that her personal information has leaked out into the open, she experiences the exact sort of apprehension and feeling of vulnerability the first category of privacy harm is concerned about. That is, she believes that there has been or could be unwanted sensing of her private information. The same is true, to a lesser degree, when any of us read about a data breach — we feel less secure in our privacy overall.
>
> But what if there is a data breach or other increased risk of adverse consequence and the "victim" never knows about it? Then there has been neither subjective nor objective privacy harm, unless or until the information is used. Worse still, it would appear on this analysis that breach notification is a net evil in that it creates (subjective) privacy harm where there would be none.
>
> Here I disagree with this premise. A risk of privacy harm is no more a privacy harm than a chance of a burn is a burn. They are conceptually distinct: one is the thing itself, the other the likelihood of that thing. A feeling of greater vulnerability can constitute privacy harm, just as the apprehension of battery can constitute a distinct tort. But there is no assault or battery without the elements of apprehension or unwanted contact. . . .

---

[18] See Rosenberg, *supra* note, at 883 (arguing that increased risk due to exposure to toxic materials is not negligence in the air but real harm due to excessive risk of diseased that is certain to take its toll on a percentage of those exposed).

[19] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms,* 96 Tex. L. Rev. — (forthcoming 2017).

> Similarly, it does not disparage the seriousness of a data breach, nor the inconvenience of having to protect against identity theft, to deny that any objective privacy harm has yet occurred. If anything, clarifying the nature of the harm at risk should help us protect against that harm actually occurring by selecting the appropriate remedy. The goal of some rules is to deter specific harms, for instance; others exist to empower the vulnerable or hinder the powerful in an effort to make harm less likely. Data breach notification laws fulfill both functions, even if they are technically the "but for" cause of one category of privacy harm.[20]

Daniel Solove examines why courts often fail to recognize harm in data breach cases:

> One of the challenges with data harms is that they are often created by the aggregation of many dispersed actors over a long period of time. They are akin to a form of pollution where each particular infraction might, in and of itself, not cause much harm, but collectively, the infractions do create harm....
>
> The flip side of collective harm is what I call the "multiplier problem," which affects the companies that cause privacy and data security problems. A company might lose personal data, and these days, even a small company can have data on tens of millions of people. Judges are reluctant to recognize harm because it might mean bankrupting a company just to give each person a very tiny amount of compensation.
>
> Today, organizations have data on so many people that when there's a leak, millions could be affected, and even a small amount of damages for each person might add up to insanely high liability....
>
> When each case is viewed in isolation, it seems quite harsh to annihilate a company for causing tiny harms to many people. . . . But that still leaves the collective harm problem. If we let it go all the time, then we have death by a thousand bee stings. . . .[21]

3. ***Emotional Distress for Lost or Stolen Sensitive Data?*** In *Beck,* the data about the Watson plaintiffs differs significantly from those about the Beck plaintiffs. In particular, the data about the Watson plaintiffs involves medical diagnoses. For these plaintiffs, is there a harm caused by the loss of this data regardless of whether there is any risk of future identity theft or fraud? If so, how would you characterize the nature of such a harm? Suppose the Watson plaintiffs sued under breach of confidentiality tort. Would they prevail?
4. ***Class Actions.*** Many of the lawsuits in the wake of data security breaches are class actions. Although many have been dismissed because courts do not recognize a harm from a mere data leak without more direct proof of injuries to plaintiffs, others have ended in multi-million dollar settlements. Defendants may choose to settle, among other reasons, due to the high expense of litigation.

   Do these class actions serving a valuable purpose? The attorneys receive a large award for attorney's fees, and class members rarely get significant benefits from the settlement. One might view class actions for data security breaches as a kind of opportunistic extortion of settlement money. On the other hand, class actions provide a strong incentive for companies to be careful with personal data and take measures to avoid data security breaches. The attorney's fees serve as an incentive for spurring lawyers to bring and litigate the case — a reward for serving as a kind of "private attorney general." If not class action litigation, is there a more appropriate mechanism to deter data security breaches?
5. ***Strict Liability for Data Security Breaches?*** Danielle Citron argues for strict liability for harms caused by data breaches. Computer databases of personal information, Citron contends, are akin to the water reservoirs of the early Industrial Age:

> The dynamics of the early Industrial Age, a time of great potential and peril, parallel those at the advent of the Information Age. Then, as now, technological change brought enormous wealth and comfort to society. Industry thrived as a result of machines powered by water reservoirs. But when the dams holding those reservoirs failed, the escaping water caused massive property and personal damage different from the interpersonal harms of the previous century. *Rylands v. Fletcher* provided the Industrial Age's strict-liability response to the accidents caused by the valuable reservoirs' escaping water. The history of *Rylands'*s reception in Britain and the United States reflects the tension between that era's desire for economic growth and its concern for security from industrial hazards.
>
> Computer databases are this century's reservoirs. . . . Much as water reservoirs drove the Industrial Age, computer databases fuel the Internet economy of our Information Age.

Citron argues that a strict liability regime is preferable to negligence tort liability:

> The rapidly changing nature of information technologies may create uncertainty as to what a negligence regime entails. . . .
>
> Due to the rapidly changing threats to information security, database operators will likely be uncertain as to what constitutes optimal care. Cyber-intruders employ increasingly innovative techniques to bypass security measures and steal personal data, thereby requiring an ever-changing information-security response to new threats, vulnerabilities, and technologies. . . .
>
> A negligence regime will fail to address the significant leaks that will occur despite database operators' exercise of due care over personal data. Security breaches are an inevitable byproduct of collecting sensitive personal information in computer databases. No amount of due care will prevent significant amounts of sensitive data from escaping into the hands of cyber-criminals. Such data leaks constitute the predictable residual risks of information reservoirs.
>
> Consequently, negligence will not efficiently manage the residual risks of hazardous databases. Negligence would neither induce database operators to change their activity level nor discourage marginal actors from collecting sensitive information because such operators need not pay for the accident costs of their residual risk. . . .

[20] M. Ryan Calo, The Boundaries of Privacy Harm, 86 Ind. L.J. 1131, 1133, 1256-57 (2011).

[21] Daniel J. Solove, Why the Law Often Doesn't Recognize Privacy and Data Security Harms, LinkedIn (July 2, 2014), https://www.linkedin.com/today/post/article/20140702054230-2259773-why-the-law-often-doesn-t-recognize-privacy-and-data-security-harms.

> Classifying database collection as an ultrahazardous activity is a logical extension of Posner's analysis. Just as no clear safety standard governing the building and maintenance of water reservoirs had emerged in the 1850s, a stable set of information-security practices has not yet materialized today. . . .
>
> In this analysis, strict liability has the potential to encourage a change in activity level respecting the storage of sensitive personal information, unless and until more information allows operators to better assess optimal precaution levels and to respond to the persistent problem of residual risk. Because strict liability would force database operators to internalize the full costs of their activities, marginally productive database operators might refrain from maintaining cyber-reservoirs of personal data. Strict liability also may decrease the collection of ultrasensitive data among those who are at greatest risk of security breaches. Moreover, as insurance markets develop in this emerging area, database operators that continue collecting sensitive information will be better positioned to assess the cost of residual risk and the extent to which they can spread the cost of such risk onto consumers.[22]

Are you convinced by the analogy between the database industry and reservoirs? Will strict liability lead to the correct level of investment in security by companies? Could it lead to over-investment in data security?

6. ***Assessing the Federal Approach to Data Security.*** As discussed above, after the ChoicePoint data security breach in 2005 — along with the numerous other breaches that followed — a majority of states have now passed data security breach legislation. Despite several proposed bills, the federal government has yet to pass a comprehensive data security law. However, some existing federal privacy laws protect data security in the context of particular industries. Consider Andrea Matwyshyn:

> The current approach to information security, exemplified by statutes such as COPPA, HIPAA, and GLBA, attempts to regulate information security by creating legal "clusters" of entities based on the type of business they transact, the types of data they control, and that data's permitted and nonpermitted uses. In other words, the current regulatory approach has singled out a few points in the system for the creation of information security enclaves. . . .
>
> The current approach ignores the fundamental tenet of security that a system is only as strong as its weakest links, not its strongest points. . . . It will not prove adequate to only ensure that a few points or clusters in the system are particularly well-secured. . . .
>
> The biggest economic losses arise not out of illegal leveraging of these protected categories of data; rather, losses arise out of stolen personally identifiable information, such as credit card data and social security numbers, which are warehoused frequently by entities that are not regulated by COPPA, HIPAA or GLBA. Therefore, creating enclaves of superior data security for data related to children online, some financial information, and some health data

[22] Danielle Keats Citron, Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age, 80 S. Cal. L. Rev. 241, 243-44, 263-67 (2007).

> will not alleviate the weak information security in other parts of the system and will not substantially diminish information crime. . . .[23]

D. FTC REGULATION

The Federal Trade Commission (FTC) has acted on numerous occasions to penalize companies that fail to take reasonable measures to protect customer data. There are several sources of authority that the FTC uses to regulate data security.

Section 5 of the FTC Act. Since the late 1990s, the FTC has concluded in more than 50 enforcement actions that companies with inadequate data security are engaging in "unfair or deceptive acts or practices" in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a). Section 5 covers a very wide array of industries, but there are a few carve outs where other statutes govern, specifically with certain types of financial institutions, airlines, and telecommunications carriers. Non-profit institutions are generally not covered by the FTC Act.

The FTC's initial enforcement actions for data security involved companies that failed to live up to promises made about data security in their privacy policies. The FTC has deemed the failure to follow statements made in a privacy policy to be a deceptive act or practice. A deceptive act or practice is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[24]

The FTC later started finding certain data security practices to be "unfair" regardless of what was promised in the privacy policy. Under the FTC Act, a practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).

In many cases, the FTC charges that a company's practices are both deceptive and unfair.

Under Section 5, the FTC lacks the authority to issue fines. When a company violates a consent decree previously entered into for a Section 5 violation, then the FTC can issue fines. Although the FTC cannot issue fines under Section 5, when it has authority under other statutes to regulate data security, some of these laws grant the FTC the ability to seek monetary penalties. Under Section 5, though, the FTC can still obtain injunctive relief. There is no private right of action for violations of Section 5 — only the FTC can enforce.

The FTC does not have specific rulemaking authority under Section 5, but it can make rules according to Magnuson-Moss rulemaking authority. This method of making rules is so burdensome that the FTC has barely used it. Instead, the FTC has focused its Section 5 efforts on enforcement.

[23] Andrea M. Matwyshyn, Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation, 3 Berkeley Bus. L.J. 129, 169-70 (2005).

[24] Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983).

Gramm-Leach-Bliley Act. The FTC can also act pursuant to its specific authority, under statutes and rules, to oversee how businesses protect consumer data. For example, the FTC's has issued the Safeguards Rule pursuant to its authority under the Gramm-Leach-Bliley Act (GLBA). The Safeguards Rule mandates data security requirements for non-bank financial institutions.

Children's Online Privacy Protection Act. The Children's Online Privacy Protection Act (COPPA) requires reasonable security for children's information collected online, and the FTC has issued a rule specifying the kinds of security provisions that companies should develop. These security obligations extend to service parties and third parties that a company uses in processing the personal information of children.

Fair Credit Reporting Act. Inadequate data security can also lead to data being disclosed impermissibly under the Fair Credit Reporting Act (FCRA). The FTC used to have primary enforcement responsibility of the FCRA, but now the enforcement is shared with the Consumer Financial Protection Bureau (CFPB), which has primary enforcement power. Fines can be issued under FCRA.

One of the most dramatic of the FTC enforcement actions for data security involved ChoicePoint. In settling the FTC charges for violating FCRA and Section 5 of the FTC Act, ChoicePoint agreed in January 2006 to pay $10 million in civil penalties and $5 million into a consumer redress fund. ChoicePoint also promised changes to its business and improvements to its security practices.

The stipulated final judgment bars the company from furnishing consumer reports to customers without a permissible purpose and requires it to establish reasonable procedures to ensure that it will provide consumer reports only to those with a permissible purpose. One requirement placed on ChoicePoint is to verify the identity of businesses that apply to receive consumer reports by auditing subscribers' use of consumer reports and by making site visits to certain of its customers.

Finally, the settlement obligated ChoicePoint to establish and maintain a comprehensive information security program and to submit this program for two decades to outside independent audits. It agreed to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." In maintaining this "comprehensive information security program," ChoicePoint promised to engage in risk assessments and to design and implement regular testing of the effectiveness of its security program's key controls, systems, and procedures. It also agreed to obtain an initial and then biennial outside assessment of its data security safeguards from an independent third-party professional.

For nearly two decades, FTC Section 5 data security cases settled. But finally, a company challenged the FTC. Wyndham Worldwide Corporation, a hotel company, argued that the FTC lacked authority under Section 5 to regulate data security and could only do so pursuant to a specific statute. Consider the case below, where the court rules on the issue.

FTC v. Wyndham Worldwide Corporation

799 F.3d 236 (3d Cir. 2015)

AMBRO, J. . . . On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation's computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges. The FTC filed suit in federal District Court, alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham's motion to dismiss, and we granted interlocutory appeal on two issues: whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision. We affirm the District Court.

Wyndham Worldwide is a hospitality company that franchises and manages hotels and sells timeshares through three subsidiaries. Wyndham licensed its brand name to approximately 90 independently owned hotels. Each Wyndham-branded hotel has a property management system that processes consumer information that includes names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes. Wyndham "manage[s]" these systems and requires the hotels to "purchase and configure" them to its own specifications. It also operates a computer network in Phoenix, Arizona, that connects its data center with the property management systems of each of the Wyndham-branded hotels.

The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." This claim is fleshed out as follows.

1. The company allowed Wyndham-branded hotels to store payment card information in clear readable text.

2. Wyndham allowed the use of easily guessed passwords to access the property management systems. For example, to gain "remote access to at least one hotel's system," which was developed by Micros Systems, Inc., the user ID and password were both "micros."

3. Wyndham failed to use "readily available security measures"—such as firewalls—to "limit access between [the] hotels' property management systems, . . . corporate network, and the Internet."

4. Wyndham allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions. It did not ensure that the hotels implemented "adequate information security policies and procedures." Also, it knowingly allowed at least one hotel to connect to the Wyndham network with an out-of-date operating system that had not received a security update in over three years. It allowed hotel servers to connect to Wyndham's network even though "default user IDs and passwords were enabled .

. . , which were easily available to hackers through simple Internet searches." And, because it failed to maintain an "adequate [ ] inventory [of] computers connected to [Wyndham's] network [to] manage the devices," it was unable to identify the source of at least one of the cybersecurity attacks.

5. Wyndham failed to "adequately restrict" the access of third-party vendors to its network and the servers of Wyndham-branded hotels. . . .

6. It failed to employ "reasonable measures to detect and prevent unauthorized access" to its computer network or to "conduct security investigations."

7. It did not follow "proper incident response procedures." The hackers used similar methods in each attack, and yet Wyndham failed to monitor its network for malware used in the previous intrusions. . . .

As noted, on three occasions in 2008 and 2009 hackers accessed Wyndham's network and the property management systems of Wyndham-branded hotels. In April 2008, hackers first broke into the local network of a hotel in Phoenix, Arizona, which was connected to Wyndham's network and the Internet. They then used the brute-force method—repeatedly guessing users' login IDs and passwords—to access an administrator account on Wyndham's network. This enabled them to obtain consumer data on computers throughout the network. In total, the hackers obtained unencrypted information for over 500,000 accounts, which they sent to a domain in Russia.

In March 2009, hackers attacked again, this time by accessing Wyndham's network through an administrative account. The FTC claims that Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges. Wyndham then discovered "memory-scraping malware" used in the previous attack on more than thirty hotels' computer systems. The FTC asserts that, due to Wyndham's "failure to monitor [the network] for the malware used in the previous attack, hackers had unauthorized access to [its] network for approximately two months." In this second attack, the hackers obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels.

Hackers in late 2009 breached Wyndham's cybersecurity a third time by accessing an administrator account on one of its networks. Because Wyndham "had still not adequately limited access between . . . the Wyndham-branded hotels' property management systems, [Wyndham's network], and the Internet," the hackers had access to the property management servers of multiple hotels. Wyndham only learned of the intrusion in January 2010 when a credit card company received complaints from cardholders. In this third attack, hackers obtained payment card information for approximately 69,000 customers from the property management systems of 28 hotels.

The FTC alleges that, in total, the hackers obtained payment card information from over 619,000 consumers, which (as noted) resulted in at least $10.6 million in fraud loss. It further states that consumers suffered financial injury through "unreimbursed fraudulent charges, increased costs, and lost access to funds or credit," and that they "expended time and money resolving fraudulent charges and mitigating subsequent harm." . . . .

Wyndham argues that a practice is only "unfair" if it is "not equitable" or is "marked by injustice, partiality, or deception." Whether these are requirements of an unfairness claim makes little difference here. A company does not act equitably

when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business. . . .

Continuing on, Wyndham asserts that a business "does not treat its customers in an 'unfair' manner when the business itself is victimized by criminals." It offers no reasoning or authority for this principle, and we can think of none ourselves. Although unfairness claims "usually involve actual and completed harms . . . they may also be brought on the basis of likely rather than actual injury." And the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs. 15 U.S.C. §45(n) ("[An unfair act or practice] causes or is *likely to cause* substantial injury" (emphasis added)). More importantly, that a company's conduct was not *the most* proximate cause of an injury generally does not immunize liability from foreseeable harms. . . .

We are therefore not persuaded by Wyndham's arguments that the alleged conduct falls outside the plain meaning of "unfair."

Wyndham next argues that, even if cybersecurity were covered by § 45(a) as initially enacted, three legislative acts since the subsection was amended in 1938 have reshaped the provision's meaning to exclude cybersecurity. A recent amendment to the Fair Credit Reporting Act directed the FTC and other agencies to develop regulations for the proper disposal of consumer data. The Gramm–Leach–Bliley Act required the FTC to establish standards for financial institutions to protect consumers' personal information. And the Children's Online Privacy Protection Act ordered the FTC to promulgate regulations requiring children's websites, among other things, to provide notice of "what information is collected from children . . ., how the operator uses such information, and the operator's disclosure practices for such information." Wyndham contends these "tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field." Citing *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000), Wyndham concludes that Congress excluded cybersecurity from the FTC's unfairness authority by enacting these measures.

We are not persuaded. The inference to congressional intent based on post-enactment legislative activity in *Brown & Williamson* was far stronger. There, the Food and Drug Administration had repeatedly disclaimed regulatory authority over tobacco products for decades. During that period, Congress enacted six statutes regulating tobacco. The FDA later shifted its position, claiming authority over tobacco products. The Supreme Court held that Congress excluded tobacco-related products from the FDA's authority in enacting the statutes. As tobacco products would necessarily be banned if subject to the FDA's regulatory authority, any interpretation to the contrary would contradict congressional intent to regulate rather than ban tobacco products outright. Wyndham does not argue that recent privacy laws *contradict* reading corporate cybersecurity into § 45(a). Instead, it merely asserts that Congress had no reason to enact them if the FTC could already regulate cybersecurity through that provision.

We disagree that Congress lacked reason to pass the recent legislation if the FTC already had regulatory authority over some cybersecurity issues. The Fair Credit Reporting Act requires (rather than authorizes) the FTC to issue

regulations, and expands the scope of the FTC's authority. The Gramm–Leach–Bliley Act similarly requires the FTC to promulgate regulations and relieves some of the burdensome §45(n) requirements for declaring acts unfair. And the Children's Online Privacy Protection Act required the FTC to issue regulations and empowered it to do so under the procedures of the Administrative Procedure Act, rather than the more burdensome Magnuson–Moss procedures under which the FTC must usually issue regulations, 15 U.S.C. §57a. Thus none of the recent privacy legislation was "inexplicable" if the FTC already had some authority to regulate corporate cybersecurity through §45(a). . . .

A conviction or punishment violates the Due Process Clause of our Constitution if the statute or regulation under which it is obtained "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." Wyndham claims that, notwithstanding whether its conduct was unfair under §45(a), the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow. . . .

Wyndham's position is unmistakable: the FTC has not yet declared that cybersecurity practices can be unfair; there is no relevant FTC rule, adjudication or document that merits deference; and the FTC is asking the federal courts to interpret §45(a) in the first instance to decide whether it prohibits the alleged conduct here. The implication of this position is similarly clear: if the federal courts are to decide whether Wyndham's conduct was unfair in the first instance under the statute without deferring to any FTC interpretation, then this case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply. The relevant question is not whether Wyndham had fair notice of the *FTC's interpretation* of the statute, but whether Wyndham had fair notice of what the *statute itself* requires. . . .

Having decided that Wyndham is entitled to notice of the meaning of the statute, we next consider whether the case should be dismissed based on fair notice principles. We do not read Wyndham's briefs as arguing the company lacked fair notice that cybersecurity practices can, as a general matter, form the basis of an unfair practice under §45(a). Wyndham argues instead it lacked notice of what specific cybersecurity practices are necessary to avoid liability. We have little trouble rejecting this claim.

To begin with, Wyndham's briefing focuses on the FTC's failure to give notice of its interpretation of the statute and does not meaningfully argue that the statute itself fails fair notice principles. We think it imprudent to hold a 100–year–old statute unconstitutional as applied to the facts of this case when we have not expressly been asked to do so.

Subsection 45(n) asks whether "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." While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity. We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls

below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute. . . .

As the FTC points out in its brief, the complaint does not allege that Wyndham used weak firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all*, did not use *any* encryption for certain customer files, and did not require some users to change their default or factory-setting passwords *at all*. Wyndham did not respond to this argument in its reply brief.

Wyndham's as-applied challenge is even weaker given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis. That said, we leave for another day whether Wyndham's alleged cybersecurity practices do in fact fail, an issue the parties did not brief. We merely note that certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court *could* find that its practices fail the cost-benefit analysis.

Several other considerations reinforce our conclusion that Wyndham's fair notice challenge fails. In 2007 the FTC issued a guidebook, *Protecting Personal Information: A Guide for Business*, which describes a "checklist[ ]" of practices that form a "sound data security plan." The guidebook does not state that any particular practice is required by §45(a), but it does counsel against many of the specific practices alleged here. . . .

Before the attacks, the FTC also filed complaints and entered into consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity. The agency published these materials on its website and provided notice of proposed consent orders in the Federal Register. Wyndham responds that the complaints cannot satisfy fair notice principles because they are not "adjudications on the merits." But even where the "ascertainable certainty" standard applies to fair notice claims, courts regularly consider materials that are neither regulations nor "adjudications on the merits." That the FTC commissioners—who must vote on whether to issue a complaint—believe that alleged cybersecurity practices fail the cost-benefit analysis of §45(n) certainly helps companies with similar practices apprehend the possibility that their cybersecurity could fail as well. . . .

NOTES & QUESTIONS

1. ***A Lack of Fair Notice?*** One of Wyndham's arguments was that the FTC's method of enforcing data security — in a case-by-case fashion rather than a rulemaking—led to companies not being put on sufficient notice about the specific data security practices that were deemed inadequate.

   Daniel Solove and Woodrow Hartzog contend that the FTC's body of consent decrees constitutes a body of law similar to the common law with

lawyers analyzing the settlements akin to the way they look at judicial decisions.[25]

In contrast, Berin Szoka and Geoffrey Manne argue that "neither this 'common law of consent decrees' nor the FTC's privacy reports constitute actual law. It's a flexible approach, but only in the worst sense: made by disposing of any legal constraints or due process."[26]

Gerard Stegmaier and Wendell Bartnick argue that a "standard based on 'reasonableness' grounded solely in settlements raises its own questions of whether constitutionally adequate fair notice was provided. Such a standard seems unfair and problematic to those tasked with assisting entities in avoiding unfair and deceptive trade practices."[27]

Hartzog and Solove contend:

> Many critics seem to want a "check list" of data security practices that will, in essence, provide a safe harbor in all contexts. Yet data security changes too quickly and is far too dependent upon context to be reduced to a one-size-fits-all checklist. Instead, the FTC has opted to defer to industry to set the appropriate standards for good data security practices by utilizing a "reasonableness" standard. . . .[28]

Hartzog and Solove point to many laws that require a reasonableness standard for data security. They further argue:

> In a common law system — or any system where matters are decided case-by-case and there is an attempt at maintaining consistency across decisions, any reasonableness standard will evolve into something more akin to a rule with specifics over time. Indeed, any broad standard will follow this evolutionary trajectory. Such a developmental pattern is inevitable if prior decisions have any kind of precedential effect or the functional equivalent of precedent. The standard will start out rather broadly, but each new case will bring a new application of that standard to a concrete situation. From these collected specific applications, the details start to accumulate around the standard's skeletal frame.[29]

2. ***Overlapping Regulatory Authority.*** After Wyndham brought its challenge, another company, LabMD, raised a similar objection to FTC authority. One of LabMD's contentions was that it is regulated by HIPAA and under the authority of the Department of Health and Human Services (HHS). Although HHS did not bring an action to enforce the HIPAA Security Rule, the FTC brought an action under Section 5 for inadequate data security. LabMD contended that because it was regulated by HIPAA, it should not fall under the FTC's Section 5 authority for data security. Assess the strength of LabMD's argument.

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

[26] Berin Szoka & Geoffrey Manne, *Now in Its 100th year, the FTC Has Become the Federal Technology Commission*, TechFreedom (Sept. 26, 2013), http://techfreedom.org/post/62344465210/now-in-its-100th-year-the-ftc-has-become-the-federal.

[27] Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 Geo. Mason L. Rev. 673 (2013).

[28] Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection,* 83 Geo. Wash. L. Rev. ___ (forthcoming 2015), http://ssrn.com/abstract=2461096.

[29] *Id.*

3. ***FTC Data Security Enforcement Under Section 5.*** Since it began enforcing Section 5 against companies for data security problems, the FTC has pursued more than 50 enforcement actions against companies for failure to provide reasonable security practices. Consider the following Congressional testimony by Woodrow Hartzog in 2014:

> The Privacy Rights Clearinghouse has reported that since 2005 there have been over 4300 data breaches made public with a total of over 868 million records breached. Yet the FTC has filed only 55 total data security-related complaints, averaging around five complaints a year since 2008.[30]

Is the number of actions sufficient? Should the FTC be more aggressively enforcing Section 5? Should a different approach be taken? Or is the FTC pursuing an appropriate amount of cases?

For example, these actions have led to settlements against Twitter, charged with bad password management practices (settlement in 2011); HTC America, charged with failure to take reasonable steps to secure tablet and phone software (settlement in 2013); and Fandago, charged with misrepresentation of its mobile applications (settlement in 2014). Consider the FTC's settlement in *Trendnet*, which involved a security camera that lacked security:

IN THE MATTER OF TRENDNET

(F.T.C. 2014)

[TRENDnet, Inc. sold a range of home networking devices. It has approximately 80 employees and $62 million in total revenue in 2012.

One of its products was a video camera that generated a live audio and video feed that users could view over an Internet connection. According to the FTC's Complaint, TRENDnet advertised the camera, named "SecurView," as a device to help consumers and small businesses monitor "babies at home, patients in the hospital, offices and banks, and more." The camera came with software that created a Web interface where the user could enter login credentials to view the live feed. The interface included an option to disable authentication, making the feed open to the public. TRENDnet also distributed Android apps that allowed users to access feeds from mobile devices.

TRENDnet had a software flaw that caused SecurView feeds to be publicly viewable even if the user had not disabled the access protections. According to the FTC Complaint, "[h]ackers could and did exploit" the vulnerability of the software. Specifically, a hacker on January 10, 2012 was able to access live feeds at Trendnet's website "without entering login credentials" and gain access to live feeds that were not intended to be public. This initial hacker posted information about the breach online and then other hackers posted links to live feeds for nearly 700 IP Cameras. The compromised live feeds allowed anyone to watch

[30] Woodrow Hartzog, *Prepared Testimony and Statement for the Record,* U.S. House of Representatives, Committee on Oversight and Government Reform (July 24, 2014).

"unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities." News stories published images from the feeds alongside photos of the locations from which the feeds were broadcast (based on geolocation of the feeds' IP addresses). Researchers discovered other security vulnerabilities, including the transmission of unencrypted passwords. TRENDnet also had failed to perform ordinary security testing.

The FTC filed a complaint against TRENDnet on January 16, 2013, alleging that TRENDnet's claims of security constituted false or misleading representations because TRENDnet failed to provide reasonable security to prevent unauthorized access to the live feeds from its cameras. As the FTC's press release accompanying the settlement of January 17, 2014 stated, "This is the agency's first action against a marketer of an everyday product with interconnectivity to the Internet and other mobile devices—commonly referred to as the 'Internet of Things.' "]

AGREEMENT CONTAINING CONSENT ORDER

The respondent, its attorney, and counsel for the Commission having executed an Agreement Containing Consent Order ("Consent Agreement"), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission's Rules. . . . .

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, other device, or an affiliate owned or controlled by respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

A. The extent to which respondent or its products or services maintain and protect:

1. The security of Covered Device Functionality;

2. The security, privacy, confidentiality, or integrity of any Covered Information; and

B. The extent to which a consumer can control the security of any Covered Information input into, stored on, captured with, accessed, or transmitted by a Covered Device. . . .

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this Order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks that could result in unauthorized access to or use of Covered Device Functionality, and (2) protect the security, confidentiality, and integrity of Covered Information, whether collected by respondent, or input into, stored on, captured with, accessed, or transmitted through a Covered Device. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device Functionality or Covered Information, including:

A. The designation of an employee or employees to coordinate and be accountable for the security program;

B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or use of Covered Device Functionality, and assessment of the sufficiency of any safeguards in place to control these risks;

C. The identification of material internal and external risks to the security, confidentiality, and integrity of Covered Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent's possession or is input into, stored on, captured with, accessed, or transmitted through a Covered Device, and assessment of the sufficiency of any safeguards in place to control these risks;

D. At a minimum, the risk assessments required by Subparts B and C should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development, and research; (3) secure software design, development, and testing; and (4) review, assessment, and response to third-party security vulnerability reports;

E. The design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including but not limited to reasonable and appropriate software security testing techniques, such as: (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Information is restricted consistent with a user's security settings;

F. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

G. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this Order, and requiring service providers, by contract, to establish and implement, and thereafter maintain, appropriate safeguards consistent with this Order; and

H. The evaluation and adjustment of the security program in light of the results of the testing and monitoring required by Subpart F, any material changes to the respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this Order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the Order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the Order for the biennial Assessments.

IT IS FURTHER ORDERED that respondent shall:

A. Notify Affected Consumers, clearly and prominently, that their Cameras had a flaw that allowed third parties to access their Live Feed Information without

inputting authentication credentials, despite their security setting choices; and provide instructions on how to remove this flaw. . . .

This Order will terminate on January 16, 2034, or [in] twenty (20) years. . . .

NOTES & QUESTIONS

1. ***The Terms of Settlement.*** This settlement illustrates the FTC's classic approach in its data security settlements of imposing long-term requirements for an information security program. Do you think that the settlement terms in *Trendnet* are appropriate? Does the FTC strike the correct balance in providing some flexibility to the companies in deciding the content of a reasonable security program? Is a 20-year enforcement period too long?
2. ***The Internet of Things***. Trendnet is the FTC's first security case involving the "Internet of Things." This term refers to Web-enabled devices that generate data, some of which can be linked to specific individuals. Cisco has already predicted 50 billion connected devices by 2020. Are there special legal challenges in regulating the privacy issues of the Internet of Things?

   A white paper by the Future of Privacy Forum (FPF), released in November 2013, argued that current implementations of Fair Information Practice Principles (FIPPs) were outdated in the new frontier of connected devices. In particular, Christopher Wolf and Jules Polonetsky, co-chairs of the FPF, point to difficulties in providing meaningful notice on devices that lack meaningful screens or user interfaces. They also question FIPPs that limit future usage of data as roadblocks to socially valuable uses of information discoverable only once data is collected. The paper proposes these new principles: (1) use anonymized data when practical; (2) respect the context in which personally identifiable information is collected; (3) be transparent about data use; (4) automate accountability mechanisms; (5) develop codes of conduct; and (6) provide individuals with reasonable access to personally identifiable information.

   Has the FPF developed principles that serve progress in information use? Or do you consider these concepts a watering-down of FIPPs?
3. ***M&A and Privacy.*** In a complaint against Reed Elsevier and its Seisint subsidiary, the FTC alleged that Reed Elsevier and Seisint failed to provide "reasonable and appropriate security to prevent authorized access" to sensitive consumer information. It argued, "In particular, respondents failed to establish or implement reasonable policies and procedures governing the creation and authentication of user credentials for authorized customers. . . ." Among other flawed practices, the FTC pointed to the companies' failure to establish or enforce rules that would make it difficult to guess user credentials. It permitted their customers to use the same word as both password and user ID. In addition, it allowed the sharing of user credentials among multiple users at a single customer firm, which lowered the likely detection of unauthorized services. Seisint also failed to mandate periodic changes of user credentials and did not implement simple, readily available defenses against common network attacks.

Reed Elsevier had acquired Seisint in September 2004 and operated it as a wholly owned subsidiary within LexisNexis, more widely known for providing legal information. The FTC privacy settlement followed in 2008. The timing of this enforcement action raises questions about merger and acquisitions for companies with possible privacy and security liability issues. What kinds of checklists should lawyers work with when advising companies that wish to merge or acquire new companies? Where do you think the greatest areas of liability are located in the privacy and security areas?

4. ***Data Leaks:*** **Eli Lilly.** In *FTC v. Eli Lilly*, No. 012-3214, the FTC charged Eli Lilly, a pharmaceutical company, with disclosing people's health data that it collected through its Prozac.com website. Prozac is a drug used for treating depression. Lilly offered customers an e-mail service that would send them e-mail messages to remind them to take or refill their medication. In June 2001, the company sent e-mail messages to all 669 users of the reminder service announcing that the service was terminated. However, this message contained the e-mail addresses of all subscribers in the "To" line of the message. The FTC alleged that the company's privacy policy promising confidentiality was deceptive because the company failed to establish adequate security protections for its consumers' data. Specifically, the FTC complaint alleged that Eli Lilly failed to

   > provide appropriate training for its employees regarding consumer privacy and information security; provide appropriate oversight and assistance for the employee who sent out the e-mail, who had no prior experience in creating, testing, or implementing the computer program used; and implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the e-mail.

   In January 2002, Eli Lilly settled. The settlement required Eli Lilly to establish a new security program. It was compelled to designate personnel to oversee the program, identify and address various security risks, and conduct an annual review of the security program. FTC Commissioners voted 5–0 to approve the settlement.

   Consider the settlements in this case and the ones described above. Do you think that these settlements are adequate to redress the rights of the individuals affected?
5. **Microsoft Passport *and* Guess*: Proactive FTC Enforcement?*** Microsoft launched Microsoft.NET Passport, an online authentication service. Passport allowed consumers to use a single username and password to access multiple websites. The goal of Passport was to serve as a universal sign-on service, eliminating the need to sign on to each website separately. A related service, Wallet, permitted users to submit credit card and billing information in order to make purchases at multiple websites without having to reenter the information on each site.

   The FTC initiated an investigation of the Passport services following a July 2001 complaint from a coalition of consumer groups. In the petition to the FTC,

the privacy groups raised questions about the collection, use, and disclosure of personal information that Passport would make possible, and asserted that Microsoft's representations about the security of the system were both unfair and deceptive. In its privacy policy, Microsoft promised that ".NET Passport is protected by powerful online security technology and a strict privacy policy." Further, Microsoft stated: "Your .NET Passport information is stored on secure .NET Passport servers that are protected in controlled facilities."

On August 8, 2002, the FTC found that Microsoft had violated § 5 of the FTC Act and announced a proposed settlement with the company. *See In the Matter of Microsoft Corp.,* No. 012-3240. The Commission found that Microsoft falsely represented that (1) it employs reasonable and appropriate measures under the circumstances to maintain and protect the privacy and confidentiality of consumers' personal information collected through its Passport and Wallet services; (2) purchases made with Passport Wallet are generally safer or more secure than purchases made at the same site without Passport Wallet when, in fact, most consumers received identical security at those sites regardless of whether they used Passport Wallet to complete their transactions; (3) Passport did not collect any personally identifiable information other than that described in its privacy policy when, in fact, Passport collected and held, for a limited time, a personally identifiable sign-in history for each user; and (4) the Kids Passport program provided parents control over what information participating websites could collect from their children.

Under the terms of the proposed consent order, Microsoft may not make any misrepresentations, expressly or by implication, of any of its information practices. Microsoft is further obligated to establish a "comprehensive information security program," and conduct an annual audit to assess the security practices. Microsoft is also required to make available to the FTC for a period of five years all documents relating to security practices as well as compliance with the orders. The order remains in place for 20 years.

The FTC took a similar approach in *In re Guess.com, Inc.,* No. 022-3260 (July 30, 2003). Guess, a clothing company, had promised that all personal information "including . . . credit card information and sign-in password, are stored in an unreadable, encrypted format at all times." This assertion of company policy was false, and the FTC initiated an action even before data was leaked or improperly accessed. The case was eventually settled.

In both *Microsoft* and *Guess*, the FTC brought an action before any data security breach had occurred. Is this a form of proactive enforcement? Suppose a company merely makes a general promise to "keep customer data secure." The FTC believes that the company is not providing adequate security and brings an action. How should the adequacy of a company's security practices be evaluated, especially in cases in which privacy policies are vague about the precise security measures taken?

6. ***The Gramm-Leach-Bliley Act and the FTC.*** Consider the following observation by Daniel Solove:

> [O]ne problem with the FTC's jurisdiction is that it is triggered when a company breaches its own privacy policy. But what if a company doesn't make explicit promises about security? One hopeful development is the Gramm-Leach-Bliley (GLB) Act. The GLB Act requires a number of agencies that regulate financial institutions to promulgate "administrative, technical, and physical safeguards for personal information." In other words, financial institutions must adopt a security system for their data, and the minimum specifications of this system are to be defined by government agencies. . . .[31]

Solove argues that the security practices of many financial institutions are quite lax, as such institutions often provide access to accounts if a person merely supplies her Social Security number. Based on the GLB Act, could the FTC use its enforcement powers to curtail such practices?

7. ***Cybersecurity and the Security and Exchange Commission (SEC).*** A new frontier for data security concerns disclosures within the context of federal security laws. A company subject to SEC requirements faces the issue of how much information to provide investors to allow them to understand the security risks that the enterprise faces. As an article by three experts in securities litigation advises: "Ultimately, the question is not whether a publicly held company should provide cybersecurity disclosures, but how it should do so effectively."[32]

Currently, there is no specific new federal disclosure standard or requirement from the SEC concerning cybersecurity disclosures. The most important policy document currently is an October 2011 Guidance from the SEC's Division of Corporation Finance. This staff guidance finds that there is no existing rule or regulation from the SEC that explicitly refers to cybersecurity risks, but a number of existing disclosure requirements may impose an obligation on SEC registrants to disclose risks and incidents. For example, in the filing of periodical reports with the SEC, such as the SEC's Regulation S-K, a registrant "should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."[33]

---

[31] Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 107-08 (2004).

[32] Howard M. Privette et al., Practice Tips, Los Angeles Lawyer (forthcoming Sept. 2014).

[33] Division of Corporate Finance, SEC, CF Disclosure Guidance: Topic No: 2, Cybersecurity (Oct. 13, 2011).