STANDING UP FOR FEDERAL DATA SECURITY LEGISLATION: A RESPONSE TO JUDICIAL CONSERVATISM IN *FERO V. EXCELLUS HEALTH PLAN, INC.*

Introduction

In *Fero v. Excellus Health Plan, Inc.*, plaintiffs brought a class action against health insurer Excellus and associated health insurance companies for a breach of Excellus's systems that exposed the personal data of 10 to 10.5 million people.[1] Plaintiffs alleged injuries from the compromise of their personally identifiable information in a data breach of the health insurer's systems, which included names, dates of birth, addresses, phone numbers, Social Security numbers, financial information, and medical insurance information.[2] In filing a 12(b)(1) motion to dismiss for lack of subject matter jurisdiction, defendants argued that plaintiffs lacked standing to bring suit.[3] The *Fero* court found standing for plaintiffs alleging actual misuse of data, but did not find standing for plaintiffs who only claimed a risk of future harm without any misuse of data.[4]

Fero addresses two salient issues of standing in data breach litigation: what is "certainly impending" to constitute an injury-in-fact and what is "fairly traceable" to show causation.[5] Post-*Clapper v. Amnesty Int'l USA*, the circuit courts split on their interpretation of what likelihood of risk satisfies *Clapper*'s "certainly impending" standard, and *Fero* adds to this dialogue with a highly conservative approach to finding imminence in the risk of future harm stemming from a breach.[6] The issue of standing at the heart of the *Fero* decision gains importance with each year as the number of data breaches increase and the number of individuals affected continues to grow.[7]

This comment will examine risk of future harm as an injury-in-fact and offer policy recommendations to address lingering issues after the *Fero* decision. Part I will provide an

overview of the data breach landscape and current standing issues in data breach litigation. Part II will outline the reasoning in *Fero* and place it within the realm of current data breach case law. Part III will provide a recommended policy remedy to address the issues of standing in data breach litigation highlighted in *Fero*.

I. Background

While the risk of identity theft is not a new phenomenon,[8] vast databases of personally identifiable information make it easy for data thieves to steal millions of identities in a single successful breach.[9] In 2017, there were over 1,200 reported data breaches in the United States.[10] Regrettably, victims of data breaches face significant barriers to accessing justice due to issues of standing that arise in the uncertainty following a breach.[11]

A. Demand Grows for Improved Data Privacy and Security

Companies, cities, and government agencies are entrusted by millions with personal information necessary to facilitate trade, government programs, and humanitarian efforts.[12] Consequently, organizations that collect, process, or maintain personally identifiable information are targets for data thieves, who seek to exploit these data troves through identity theft, unauthorized credit card use, fraudulent accounts, medical ID theft, and tax fraud.[13] Identity theft can also incur additional injuries resulting from an affected credit report, including inability to obtain a mortgage or loan, denial of rental housing applications, and rejection from employment opportunities.[14] Between the costs of repair, notification, state suits, and consumer class actions, a single data breach can cost a company millions.[15]

Global data sharing poses a significant threat to individuals' privacy and security—one that will require international cooperation.[16] While there is no international consensus on privacy standards, many nations are strengthening their data laws, and consequently, requiring similar

standards of countries with whom they are engaged in data exchange.[17] Notably, the European Court of Justice made a clear statement in *Schrems v. Data Protection Commissioner* that the United States lacked adequate privacy standards and enforcement by invalidating the Safe Harbour Principles that had previously governed their exchange of personal data with the United States.[18]

B. Standing in Data Breach Litigation

Individuals seeking redress for their injuries resulting from a data breach—including risk of future identity theft, anxiety, and time spent mitigating damages—face obstacles in establishing standing to bring suit.[19] Standing emerges from separation of powers principles articulated in the Constitution that limit judicial authority to cases and controversies.[20] This prevents the judiciary from exercising power that is unchecked by democratic processes.[21] Standing is "a party's right to make a legal claim or seek judicial enforcement of a duty or right."[22] To establish standing, a litigant must satisfy three elements: injury-in-fact, causation, and redressability.[23]

The Supreme Court has considered issues of standing in two recent decisions that affect data breach litigants.[24] In *Clapper v. Amnesty Int'l USA*, the Supreme Court affirmed use of the "certainly impending" standard to determine whether an injury is sufficiently imminent to satisfy the "actual or imminent" injury-in-fact requirement.[25] However, the circuits quickly split on their interpretations of the standard because the Court did not specify what likelihood of occurrence satisfied the standard.[26] Three years later, the Court took up the issue of standing again in *Spokeo v. Robins*, where it elaborated on the "concrete and particularized" element of the injury-in-fact requirement.[27] However, despite the circuit split in the evaluation of injury in data breach cases

to constitute standing, the Supreme Court failed to take up the issue when it denied certiorari in *Attias v. CareFirst*.[28]

Fero signals that courts will likely continue to apply varying standards of imminence in data breach suits unless action is taken by the Supreme Court to clarify the imminence standard, or federal data breach legislation is passed that defines what constitutes an injury under the law. Until then, parties in data breach litigation will vie for jurisdiction in circuits that apply the most favorable interpretation of standing to their position, and consequently, cases with similar facts may continue to receive divergent outcomes.[29]

II. Case Description

In *Fero v. Excellus Health Plan, Inc.*, the Western District of New York followed the First and Third Circuits in applying a conservative approach to imminence under *Clapper*.[30] The court differentiated the case from Sixth and Seventh Circuit cases that involved an "identifiable taking" of personal information.[31] *Fero* could provide the Second Circuit with an opportunity to reconsider the subject after issuing a non-precedential standing decision in *Whalen v. Michaels Stores, Inc*.[32]

On a motion to dismiss on the grounds that plaintiffs lacked standing, defendants challenged that 1) plaintiffs who did not allege misuse of data could not prove that the risk of future harm was "certainly impending"[33] and 2) plaintiffs alleging misuse of data could not prove that the misuse was "fairly traceable" to the breach.[34] After analyzing the facts of the case under *Clapper*, the court did not find standing for plaintiffs without actual misuse of personal data because an investigation did not conclusively show that the data had been appropriated by the hackers.[35] Without finding the information had in fact been stolen, the court found the risk of future identity theft speculative and not "certainly impending."[36] The court further narrowed the

meaning of "certainly impending" or "substantial risk"[37] in finding that instances of identity theft among some class members are not enough to prove risk of future harm for other class members.[38] The court also found plaintiffs' alternative bases for standing insufficient, including injuries due to mitigation efforts, [39] overpayment for services, and diminution in value of information.[40]

III. Analysis

Cases like *Fero*—that narrowly define imminence and further curtail victims' ability to seek redress for data breach injuries— demonstrate the need for comprehensive data security legislation to provide a clear avenue for data breach victims to hold organizations accountable when they fail to adequately protect their personal information. An identity cannot expire, be exchanged, or diminish in value, and for these reasons, it is priceless to its owner.[41] When compromised in a data breach, certain personal information can create a lifelong risk of identity theft.[42] Organizations that store personal data should have a duty to those who have entrusted them with their information, and consequently, organizations should bear the responsibility for breaching that duty when they have insufficient safeguards in place to protect this information from hackers.[43]

A. Patchwork Legislation and Regulation Fail to Adequately Enforce Individual Rights

States have clearly signaled that data security is important; 48 states have laws governing the disclosure of data breaches.[44] State data breach disclosure laws incentivize organizations that store personal data to institute better safeguards against a possible breach and result in better protection of consumer information.[45] However, breach disclosure laws' "focus on notification makes them a poor avenue for consumers seeking remedial action. . . . [I]t is unlikely to result in any redress for individuals . . . as many of these statutes lack a private right of action."[46]

The Federal Trade Commission (FTC) also has the authority to regulate data security issues under the FTC Act. Notably, in an adjudication before the FTC, Google was ordered to maintain a privacy program containing "privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information."[47] Google was also ordered to undergo biennial assessments conducted by a qualified, independent third party to report on the adequacy and efficacy of company privacy controls in meeting the privacy program's requirements.[48] But again, like state disclosure laws, agency enforcement is unlikely to address the individual concerns of consumers because the agency cannot issue civil penalties and the Act does not authorize citizen suits.[49]

B. Stronger Consumer Data Protection Laws Are Necessary to Satisfy International Standards

From human rights to global commerce, international relations rely on strong data privacy and security, and federal legislation will be necessary to maintain these relationships. Following on the heels of the *Schrems* decision invalidating Safe Harbour, FTC Commissioner Julie Brill told European Union members that the agency had called for "more robust consumer privacy laws," federal data security legislation, and "baseline privacy legislation" for sensitive information that does not fall under the current protections of financial, medical, or credit data.[50] In the meantime, however, no such legislation has passed, while E.U. data security requirements have continued to move forward with the progress of the E.U. General Data Protection Regulation.[51] Data security is a crucial issue concerning governments around the world, and the United States should take steps to show that it is serious about addressing this issue by passing federal legislation.

C. Comprehensive Federal Legislation Is the Answer

Attempts to pass federal data security legislation have repeatedly failed despite the clear need for action.[52] However, efforts to craft comprehensive legislation forge ahead despite these setbacks.[53] Implementing a federal legislative solution would not only clarify organizations' data security responsibilities, but also allow them to anticipate and mitigate potential liability.[54] Legislation would also protect consumers and their personal information, reduce uncertainty following a data breach, and ensure victims of data breaches are able to vindicate their rights in court.

Imposing a Duty of Care Would Allow Individuals to Seek Redress for Breach of Duty

Organizations that store personal information should owe a duty of care towards individuals who entrust them with their data, and plaintiffs should be able to bring an action for breach of that duty when their information is improperly accessed due to insufficient security protections. In drafting comprehensive data security legislation, Congress should look to existing federal and state laws that impose a duty of care on data keepers[55] and recognize individuals' rights to safety and privacy.[56] To ensure data breach victims have the ability to use the courts to vindicate their rights, it is necessary for the legislature to articulate a duty of care that data keepers owe to consumers and the public and define the injury of future harm that arises from a breach.[57] Any legislation should also include a citizen suit provision to allow individuals to enforce their rights in court.

Granting Authority to the FTC to Promulgate Rules Related to Data Security Would Clarify Data Keepers' Responsibilities Under the New Law

In light of a newly defined duty of care, both large and small businesses would benefit from clear standards for data security.[58] With a set of standards for data security, businesses

could limit their liability by meeting the standard. Beyond system protection requirements, standards would also address methods for disposal, such as the U.N. recommendations that organizations should dispose of excess data from inactive users.[59] By setting standards for disposal, data keepers could limit their liability, and individuals would be protected from breaches involving information they were not even aware was still in the care of the organization. [60]

Under a new data security law, Congress should grant authority to the Federal Trade Commission to impose standards for data security. The FTC has experience enforcing data security in the context of unfair and deceptive business practices under the FTC Act and would be well-equipped to apply its considerable expertise to rulemaking under this new legislation.[61] While there are concerns that uniform federal standards would "water down" security requirements, [62] granting authority to the FTC to promulgate rules under the new legislation would not preclude the issuance of industry-specific rules to address the unique data requirements in the medical and finance sectors.

Defining "Personally Identifiable Information" Narrowly Would Encourage Protection of Sensitive Information Without Opening the Floodgates of Liability

In creating a statutory basis for injury in data breaches, personally identifiable information under the statute should be defined narrowly to limit data keepers from being liable for all types of personal data, whether or not it actually exposes the individual to an increased risk of identity theft. Sensitive personal information, social security numbers, medical information, and financial information are data categories that create a serious risk of future harm that can last well beyond the statute of limitations.[63] States have taken different approaches to defining personal information under their data breach notification statutes. For example, both

Colorado and Massachusetts have defined personal identifying information under these categories.[64] Some courts have ruled that financial information does not qualify as a substantial risk of harm unless the breach involves other personal information because it "generally cannot be used alone to open unauthorized new accounts."[65] However, these cases do not consider the effect of data aggregation, where the risk of an individual breach is compounded by the availability of victims' personal information data from previous breaches that could allow data thieves to compile the data.[66]

Creating a Minimum Recovery Under Statute for Medical Data Breaches Would Incentivize Better Protection

In 2015, the medical sector brought 37 percent of all data breach class action lawsuits.[67] Medical identity theft "can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs."[68] Generally, most breaches involving medical information arise from theft, as opposed to hacking, unauthorized access, or improper disposal.[69] In *Adobe Sys., Inc. Privacy Litig.*, the court found theft sufficient to prove that the risk of future harm from the data breach was "certainly impending."[70] The high rate of medical data theft indicates a market for medical information and underscores the need to incentivize its protection.

The pervasiveness of medical data breaches and serious consequences of medical identity theft support the critical need to protect medical information. Injuries resulting from a breach can vary and can be difficult to account for when considering non-monetary costs, such as time spent mitigating damages and anxiety due to a reasonable fear of identity theft.[71] In a non-data breach case, *In re Currency Conversion Fee*, the issue of variability in damage awards was addressed by awarding a base amount to each claimant, and allowing those who could prove greater damages

to do so.[72] This solution could be applied to breaches involving medical data to offer plaintiffs compensation for a risk of future harm that could potentially continue throughout their lifetime and to incentivize data keepers to implement better safeguards to protect this valuable information that can have life or death consequences.

Conclusion

Data breaches present a serious threat to the privacy and security of personal information; the records of millions of individuals are capable of being exposed in a single data breach, and the number of breaches are growing every year. Yet data breach victims continue to face significant barriers to seeking redress for their injuries. As was the case in *Fero*, victims are frequently unable to meet the injury-in-fact standing requirement based on the court's interpretation of the imminence of a risk of future harm.

However, where the courts are unwilling to tread, Congress can and should. Enacting federal data security legislation would aid plaintiffs by establishing a duty of care and clearly defining an injury that meets the case and controversy requirement under Article III.

[1] Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 46 (W.D.N.Y. 2017).

[2] *Id.* at 744.

[3] *Id.* at 743.

[4] *Id.* at 759.

[5] *Id.* at 744.

[6] *Id.* at 749.

[7] Ifrah PLLC, *The Data Breach Legal Limbo on Consumers' Ability to Sue Hacked Companies*, FTC BEAT (Jan. 16, 2018), https://www.jdsupra.com/legalnews/the-data-breach-legal-limbo-on-62346/ ("The Identity Theft Resource Center reported that there were some 1,202 breaches in the 11 months to November 2017, up ten percent from 2016."); Patrick J. Lorio, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 81 (Fall 2017) ("[I]n recent years . . . the size and scope of data breaches of major corporations have steadily increased. This trend is expected to continue as hackers become increasingly sophisticated and more personal information is stored digitally.").

[8] *See, e.g.*, S.M. Furnell & M.J. Warren, *Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?*, 18 COMPS. & SEC. 1, at 28 (1999); *Genesis* 27 (King James) (Jacob's impersonation of his brother Esau tricked their father into blessing him instead of Esau).

[9] Fed. Trade Comm'n, The Equifax Data Breach: What to Do (Sept. 8, 2017) (exposing 143 million people's names, birth dates, addresses, social security numbers, and some credit card and driver's license numbers); *see generally* Edvard Pettersson, *Equifax May Be Happy Paying $1 per Customer for Their Hassle*, BLOOMBERG (Sept. 20, 2017 4:00 AM),

https://www.bloomberg.com/news/articles/2017-09-20/equifax-may-be-happy-to-spend-1-per-customer-for-their-trouble (concerning Equifax's potential $143 million liability for the breach).

[10] Ifrah PLLC, *supra* note 7 ("The Identity Theft Resource Center reported that there were some 1,202 breaches in the 11 months to November 2017, up ten percent from 2016.").

[11] Daniel J. Solove & Danielle Keats, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 4, at 737, 58 (2018) ("[I]ronically the very factors that make identity theft so harmful—the difficulty in catching the perpetrators and the fact that it can continue indefinitely—are what impede victims' ability to obtain redress in the courts.").

[12] *See, e.g.*, Amanda Bronstad, *Regulators, Not Class Actions, Could Drive Legal Response to Uber Data Breach*, RECORDER (Nov. 29, 2017 8:23 PM), https://www.law.com/therecorder/sites/therecorder/2017/11/29/regulators-not-class-actions-could-drive-legal-response-to-uber-data-breach/ (Uber data breach in 2016 exposed the records of 57 million people and included names, emails, and driver's license numbers); *Officials Say Residents' Data Possibly Hacked in Data Breach* (Fox 5 Atlanta television broadcast Mar. 27, 2018), https://www.youtube.com/watch?v=TVkJZwEjdh8 (involving personal and financial information in city servers used for property taxes, utility payments, and other city services).

[13] Adam Shell, *Equifax Data Breach Could Create Lifelong Identity Theft Threat*, USA TODAY (Sept. 9, 2017), https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/.

[14] Solove & Keats, *supra* note 11, at 759.

[15] *E.g.*, Reuters, *Target Settles 2013 Hacked Customer Data Breach for $18.5 Million*, NBC NEWS (May 24, 2017 10:49 AM), https://www.nbcnews.com/business/businessnews/target-

settles-2013-hacked-customer-data-breach-18-5-million-n764031 (total cost of 2013 Target breach was $202 million).

[16] *See generally* U.N. Dev. Grp., Data Privacy, Ethics, and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda, http://www.undg.org.

[17] *Id.* at 10; Schrems v. Data Protection Comm'r, 2015 E.C.R. C-362/14, at 650 ¶ 19 (as of Sept. 2013, 3,246 companies were certified under Safe Harbour principles governing U.S. companies who receive E.U. citizens' personal data); *see, e.g.*, Data Privacy Act of 2012, Rep. Act No. 10173, §§ 3–5 (Aug. 15, 2012) (Phil.).

[18] *Schrems*, 2015 E.C.R. ¶ 15 (invalidating Safe Harbour due to weak enforcement in the United States and mandatory "surrender of data to U.S. intelligence agencies.").

[19] Daniel R. Stoller, *SuperValu Data Breach Claim Nixed, Court Sees No Consumer Harm*, BLOOMBERG L. (Mar. 8, 2018), https://www.bna.com/supervalu-data-breach-n57982089668/.

[20] U.S. CONST. art. III; THE FEDERALIST NO. 78 (Alexander Hamilton) ("The interpretation of the laws is the proper and peculiar province of the courts. A constitution is . . . a fundamental law. It therefore belongs to [the judiciary] to ascertain its meaning.").

[21] Martin H. Redish & Sopan Joshi, *Litigating Article III Standing: A Proposed Solution to the Serious (But Unrecognized) Separation of Powers Problem*, 162 U. PA. L. REV. 1373, 84 (May 2014).

[22] *Standing*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[23] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) ("To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139 (2010)).

[24] *Id.*; Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

[25] *Clapper*, 568 U.S. at 409 ("'Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes.'" (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 565 (1992))).

[26] *Compare* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 93 (7th Cir. 2015) ("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 a fraudulent charge or assume those consumers' identities."), *and* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 88 (6th Cir. 2016) ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for . . . fraudulent purposes."), *with* Beck v. McDonald, 848 F.3d 262, 75–76 (4th Cir. 2017) ("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.").

[27] *Spokeo*, 136 S. Ct. at 1549–50 ("Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, Robins could not . . . allege a bare procedural violation, divorced from any concrete harm. . . . [T]he violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact . . . . [but] a violation of . . . procedural requirements *may* result in no harm."); *see* Merritt Baer & Chinmayi Sharma, *Your Voter Records Are Compromised. Can You Sue? Theories of Harm in Data-Breach Litigation*, LAWFARE (Aug. 7, 2017 11:03 AM), https://lawfareblog.com/your-voter-records-are-compromised-can-you-sue-theories-harm-data-breach-litigation/ ("[T]he 3rd Circuit concluded

that a violation of the Federal Credit Report [sic] Act . . . amounted to injury even without an additional showing of harm because the very purpose of the law was to prevent the wrongful disclosure of personal information.").

[28] Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, CareFirst, Inc. v. Attias, 138 S. Ct. 981 (2018); *see* Paul Roberts, *Supreme Court Could Decide Question of "Harm" in Data Breaches*, DIGITAL GUARDIAN (Nov. 16, 2017), https://digitalguardian.com/blog/supreme-court-could-decide-question-harm-data-breaches; John K. Higgins, *Consumers Gain More Power to Seek Data Breach Damages*, E-COMMERCE TIMES (Aug. 21, 2017 1:43 PM), https://www.ecommercetimes.com/story/84747.html.

[29] *Compare* Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735 (W.D.N.Y. 2017) (finding no standing for plaintiffs who had medical data accessed), *with CareFirst*, 865 F.3d at 620 (finding a "substantial risk" exists for plaintiffs whose medical information was hacked "simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.").

[30] *Fero*, 236 F. Supp. 3d at 49–53.

[31] *Id.* at 750–51.

[32] Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017) (summary order finding no risk of future identity theft because plaintiff promptly canceled credit card after financial information was compromised and the breach did not include additional personally identifiable information); 2d Cir. R. 32.1.1 (rulings by summary order do not have precedential effect).

[33] *CareFirst*, 865 F.3d at 748.

[34] *Id.* at 746.

[35] *Id.* at 753.

[36] *Id.*

[37] Clapper v. Amnesty Int'l USA, 568 U.S. 398, n.5 (2013) ("Our 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 harm will occur . . . . But to the extent that the "substantial risk" standard . . . is distinct from the "clearly impending requirement, respondents fall short of even that standard.").

[38] *Id.* at 748.

[39] *Id.* at 754 ("[M]itigation efforts following a data breach do not confer standing where the alleged harm is not imminent." (citing Beck v. McDonald, 848 F.3d 262, 75–76 (4th Cir. 2017))).

[40] *Id.* at 754–55.

[41] Shell, *supra* note 13; *see also* WILLIAM SHAKESPEARE, OTHELLO act 3, sc. 3.

[42] Shell, *supra* note 13.

[43] Lorio, *supra* note 7.

[44] Louise Matsakis, *Uber "Surprised" by Totally Unsurprising Pennsylvania Data Breach Lawsuit*, WIRED (Mar. 5, 2018 5:52 PM), https://www.wired.com/story/uber-pennsylvania-data-breach-lawsuit/; *see, e.g.*, CAL. CIV. CODE § 1798.8–.82 (2018); 201 MASS. CODE REGS. 17.

[45] Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANAL. & MGMT. 2, at 256, 60 (2011) ("adoption of [data breach] disclosure laws reduces identity thefts, on average, by 6.1%."); Ravi Sen & Sharad Borle, *Estimating the Contextual Risk of Data Breach: An Empirical Approach*, 32 J. MGMT. INFO. SYS. 2, at 314 (2015).

[46] John Biglow, Note and Comment, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943, 73 (Spring 2016).

[47] Complaint, Google, Inc., No. C-4336, at *9 (F.T.C. Oct. 13, 2011), 2011 WL 5089551 (F.T.C.).

[48] *Id.* at 10.

[49] *Id.* at 960.

[50] Julie Brill, Comm'r, Fed. Trade Comm'n, Remarks at the 6th Annual Privacy and Data Protection Conference, *5 (Dec. 10, 2015), 2015 WL 9684102 (F.T.C.).

[51] Ifrah PLLC, *supra* note 7.

[52] *E.g.*, PERSONAL DATA PRIVACY AND SECURITY ACT OF 2009, S. 1490, 111th Cong. (2009); Matsakis, *supra* note 44 ("In December [2017], Democratic senator Bill Nelson introduced the Data Security and Breach Notification Act, which would require companies to report breaches within a month, or face up to five years in prison."); *see also* Kim Zetter, *National Data Breach Laws Move Through Senate*, WIRED (Nov. 6, 2009 5:29 PM), https://www.wired.com/2009/11/breach-laws/ (discussing the proposed Personal Data Privacy and Security Act of 2009).

[53] Matsakis, *supra* note 44.

[54] *E.g.*, Brief for Chamber of Commerce of the United States as Amicus Curiae Supporting Appellees, Attias v. CareFirst, No. 16-7108, *23-26 (D.C. Cir. Feb. 15, 2017), 2017 WL 632533 ("[I]n terrorem settlements . . . impose substantial costs on businesses even in the absence of real-world injury. . . . American businesses spend an average of $6.5 million on a single data breach." (quoting Institute for Legal Reform, Data Privacy, http://www.instituteforlegalreform.com/issues/data-privacy)); PONEMON INSTITUTE, 2013 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 1–2 (May 2013) (finding the United States spent, on average, $188 per record for malicious attacks and $277 per record compromised in 2013).

[55] Privacy Act of 1974, 5 U.S.C. § 552a(e)(10) (2016) (requiring agency safeguards for the security and confidentiality of records).

[56] CAL. CONST. art. 1, § 1 (recognizing a right to safety and privacy).

[57] Jordan Z. Dillon, *Standing on the Wrong Foot: The Seventh Circuit's Eccentric Attempt to Rescue Risk-based Standing in Data Breach Litigation*, 56 WASHBURN L.J. 123, 30 (Winter 2017) ("In data breach situations, the transition from data breach to identity theft depends on third party actions, which are inherently speculative.").

[58] Eric Cernak, *Why Data Theft Poses a Big Risk to Small Businesses*, USA TODAY (May 6, 2013), https://www.usatoday.com/story/cybertruth/2013/05/06/data-breach-small-business-cybersecurity-online-privacy/2138713/ (55% of small businesses have had a data breach); Mark Zuckerberg, FACEBOOK (Mar. 21, 2018 2:36 PM), https://www.facebook.com/zuck/posts/10104712037900071 (instituting policies for third party data sharing to minimize impact of future breaches).

[59] U.N. Dev. Grp., s*upra* note 16, at 6 ("Data access, analysis or other use should be kept to the minimum amount necessary to fulfill its purpose. . . . Any retention of data should have a legitimate and fair basis . . . to ensure that no extra or just-in-case data set is stored.").

[60] Benjamin Schwartz, Cartoon, NEW YORKER (Sept. 23, 2016), https://www.newyorker.com/cartoon/daily-cartoon-092316-yahoo.

[61] Complaint, Google, Inc., No. C-4336, at *9 (F.T.C. Oct. 13, 2011), 2011 WL 5089551 (F.T.C.) (ordering Google to institute a comprehensive privacy program requiring "the identification of reasonably foreseeable, material risks . . . an assessment of the sufficiency of any safeguards in place to control these risks . . . the design and implementation of reasonable

privacy controls and procedures to address the risks . . . and regular testing or monitoring of [their] effectiveness.").

[62] Matsakis, *supra* note 44 ("'I would be skeptical of the claims that a unified data security protection law are going to provide clarity and better data protection at the same time,' says [Woodrow] Hartzog, who has testified before Congress about data breach legislation. 'A movement to have a single unified standard among the United States would be seen as an opportunity to water down those requirements.'").

[63] Solove & Keats, *supra* note 11, at 758–64; Claire Wilka, Note, *The Effects of Clapper v. Amnesty International USA: An Improper Tightening of the Requirement for Article III Standing in Medical Data Breach Litigation*, 49 CREIGH. L. REV. 467, 68 (Mar. 2016).

[64] COLO. REV. STAT. § 6-1-713 (2018); 201 MASS. CODE REGS. 17.

[65] *In re* Supervalu, Inc., 870 F.3d 763, 70 (8th Cir. 2017) (quoting U.S. Gov't Accountability Office, GAO-07-737, Report to Congressional Requesters: Personal Information 29 (2007)); *accord* Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017) (finding no standing where financial information was stolen without additional personally identifiable information); Petition for Rehearing En Banc, Remijas v. Neiman Marcus Grp., No. 14-3122 (7th Cir. Aug. 3, 2015), 2015 WL 4639951 ("[T]he risk of broader identity theft from compromise of payment card data held by a retailer is small.").

[66] Solove & Keats, *supra* note 11, at 775 (assessing risk based on extent information can be aggregated to result in harm).

[67] Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Cases*, WALL ST. J. (June 26, 2016 8:06 PM), https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-14669859988.

[68] Attias v. CareFirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017), *cert. denied*, CareFirst, Inc. v. Attias, 138 S. Ct. 981 (2018) (quoting J.A. 12).

[69] Vincent Liu et al., *Data Breaches of Protected Health Information in the United States*, 313 J. AM. MED. ASS'N 14, at 1471, 72 (Apr. 14, 2015).

[70] *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) ("[H]ere there is no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken. . . . Not only did the hackers deliberately target Adobe's servers, but . . . hackers used Adobe's own systems to decrypt customer credit card numbers.").

[71] Megan Dowty, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 709 (Mar. 2017) ("The range of time and resources spent sorting out one's finances after a breach can vary greatly. More than half (52%) of the 17.6 million identity theft victims in 2014 'were able to resolve any problems . . . in a day or less, while about 9% spent more than a month.'" (citing BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ248991, VICTIMS OF IDENTITY THEFT, 2014 (2015), http://www.bjs.gov/content/pub/pdf/vit14_sum.pdf.)).

[72] *Id.* at 712. ("[A]ll claimants received a minimum of twenty-five dollars by simply being a member of the damages class. But if a plaintiff could prove higher damages, that plaintiff could prove actual damages. . . . A [similar] payout structure . . . could be used in data breach actions to account for the variability plaintiffs are likely to experience in damages." (citing *In re* Currency Conversion Fee Antitrust Litig., 263 F.R.D. 110, 115 (S.D.N.Y. 2009))); *C.f.* Video Privacy Protection Act, 18 U.S.C. § 2710 (2013) (civil suit provision and minimum recovery of $2500 if court deems personal data was knowingly disclosed).