EVERYONE IS CONFUSED & NO ONE IS HAPPY: CRITIQUING RULES AND RESULTS IN *FERO V. EXCELLUS HEALTH PLAN, INC.* AND ARGUING FOR A NEW APPROACH TO DATA BREACH STANDING

Introduction

The plaintiffs in *Fero v. Excellus Health Plan, Inc.* ("*Excellus*") were among millions of individuals whose personally identifiable and protected health information was compromised when Excellus Health Plan, Inc.'s computer network was breached from December 2013 to August 2014.[1] After being notified by Excellus that their information was compromised, consumers filed several class action lawsuits over alleged present and future injuries. In response, the defendants, Excellus and its affiliates, filed motions to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1).[2] The court dismissed claims by plaintiffs who did not allege past misuse of their information because the alleged increased risk of future identity theft was not sufficiently imminent to satisfy the injury in fact requirement for Article III standing.[3]

Whether data breach victims have Article III standing under current doctrine depends on factual differences between cases[4] and legal differences between courts.[5] These variations are important because they determine whether a case can proceed to the merits,[6] which in turn can impact business conduct.[7] *Excellus* highlights the breadth of the circuit split on both injury in fact within standing doctrine, and the standard of review for questions of standing overall. It is notable because, at the time, the Second Circuit Court of Appeals had not decided a data breach case, so the position of the circuit was unknown.[8] The district court was challenged to form its own standing rule for data breach litigation.

This Comment considers the quality of precedent set by *Excellus* by critiquing the legal reasoning and analyzing the impact of the results. Part I surveys standing doctrine and injury in

fact theory as applied to data breach litigation. It then contemplates data security enforcement outside the courts. Part II takes a deeper dive into the court's reasoning and holding in *Excellus*. Part III examines the court's decision from analytical and policy perspectives, and in light of the subsequent *Attias v. CareFirst, Inc.* decision by the D.C. Circuit Court of Appeals that almost went to the Supreme Court. This comment concludes that *Excellus* created an arbitrary standard because the legal rule applied is ambiguous and incomplete. The resulting uncertainty for redress and liability illustrates the need for legislative or judicial action to clarify data breach standing.

I. BACKGROUND

The horror of identity theft is nothing new[9] but the prevalence of data breaches and addressing them in court is a relatively new and confounding reality.[10] Protecting individuals from identity theft is a significant concern, particularly because the risk from stolen data can last long after a breach.[11] Data breaches are an issue for organizations of all types[12] but the impact differs by industry, with health care breaches being most costly.[13] Lawsuits against a hacked entity can accumulate quickly after a data breach is disclosed.[14] Businesses may settle these lawsuits readily, or push back against misplaced blame.[15]

A. Standing Doctrine and Injury in Fact

The first hurdle data breach lawsuits face is whether the case can proceed to the merits, due to prerequisites to sue in federal court.[16] Standing doctrine is a set of principles to determine whether federal courts have jurisdiction to hear a case derived from the Case or Controversy Clause of Article III of the Constitution.[17] It is often distilled to three elements: "a plaintiff must show that she has suffered an 'injury in fact' that is 'fairly traceable' to the defendant's actions and that is 'likely to be redressed' by the relief she seeks."[18] These requirements encapsulate protections for the separation of powers, a concern since the courts were established.[19] However,

the current articulation of standing developed in the 20th century.[20] The most contentious facet of standing doctrine in data breach litigation is the injury in fact requirement because claims are often for increased risk of future injury.[21] Plaintiffs may also claim present injury due to mitigation efforts or anxiety or fear about potential identity theft.[22] However, most courts are reluctant to grant standing for these allegations though without an accompanying justiciable risk of future injury.[23]

Future injury confers standing if it is "certainly impending" or constitutes a "substantial risk" to the plaintiff.[24] *Clapper v. Amnesty International, USA*, the main case on future injury from the Supreme Court, illustrates one scenario in which an alleged future injury does *not* confer standing.[25] The facts were extenuating though, as it was a constitutional challenge to legislative action regarding foreign affairs, an area where the Court avoids deciding the merits.[26] Without an example of what *is* future injury in fact, and faced with precedent from unusual circumstances, courts struggle to extrapolate the rule to the data breach litigation, leading to the circuit split.[27]

B. Injury in Fact in Data Breach Litigation Across Jurisdictions

Each jurisdiction has different positions on injury in fact, some based in law, others viewed as fact-specific.[28] A purely legal disagreement between circuits is the proper standard of review for Rule 12(b)(1) motions to dismiss for lack of subject matter jurisdiction.[29] Many courts apply the standard from *Lujan v. Defenders of Wildlife*, which only requires general allegations of each element of standing at the pleading stage.[30] The standard of review in turn affects the courts propensity to draw inferences[31] regarding the malice of data breaches and the likelihood of fraud.[32] The type of data exposed may impact judgment regarding the magnitude of the risk,

since sensitive information such as social security numbers can be wielded more harmfully.[33] Imminence may be indicated by evidence that data was targeted specifically.[34]

The Supreme Court has yet to weigh-in directly on future injury in the data breach context. It recently surprised the legal community[35] by denying a petition for writ of certiorari on *Attias v. CareFirst, Inc.*[36] In that case, the D.C. Circuit Court of Appeals held that "a substantial risk of harm exists . . . simply by virtue of [a] hack and the nature of the data."[37] The court reversed because the data included both social security numbers and medical information, which even the defendants allegedly viewed as creating a substantial risk of identity theft.[38] While denying certiorari is not the same as deciding a case outright, the refusal could indicate the Court either assents to the lower court's rule or does not think the circuit split is problematic.

C. Legislative and Government Actions to Address Data Security

All but two states have legislation requiring at least disclosure of data breaches to consumers, [39] if not additional preventative requirements.[40] Criticism of existing legislation includes that it does not improve data security[41] nor help consumers because there is no redress available through notification.[42] Businesses may not even be aware of the requirement,[43] or realize the breach too late to give consumers enough notice to prevent identity theft.[44] From the business perspective, notification requirements increase the cost of a data breach.[45]

There are some federal mechanisms to increase data security, but no nationwide legislation governing private entities.[46] The push to introduce federal data breach prevention and response legislation ebbs and flows.[47] Despite the desire to prevent data breaches and avoid identity theft,[48] there are competing interests, conflicting priorities,[49] and varying views on how to improve data security.[50] Furthermore, even if there was a federal law including a cause of action, it is unclear whether it would be able to provide civil remedies.[51] It is also arguable

whether a statute would create better incentives for responsible data storage than current state laws, FTC monitoring and adjudication,[52] and overall trends.[53]

However, there are strong arguments for and possible benefits to legislation, not least of which are related to international relations, trade and commerce, and national security.[54] To stay relevant with global allies, the United States may have to increase its involvement in data security and breach response to stay relevant, as indicated by recent European Union action and illustrated by international standards.[55] Regarding standing, legal scholarship suggests legislation is the proper way to allocate risk and make trade-offs related to ubiquitous consumer data collection.[56] Legislation could create statutory standing, relieving concerns about courts loosening Article III standing requirements.[57] Legislation could also improve outcomes for businesses currently mired in the standing circuit split by increasing certainty about liability.[58]

II. CASE DESCRIPTION

Four of twenty named plaintiffs in *Fero v. Excellus Health Plan, Inc.* did not allege specific misuse of their personal data exposed since the cyberattack.[59] Their alleged injuries mirrored typical complaints: increased risk of future injury, anxiety and fear related to the possibility of future identity theft, and effort exerted to take precautions against identity theft. The claims were pursuant to myriad causes of action, including some arising from tort and contract law, as well as state statutes.[60] The district court decided the motion to dismiss for lack of subject matter jurisdiction based on a preponderance of the evidence standard, with consideration of evidence outside the pleadings.[61] The court discerned a rule for injury-in-fact from non-binding precedent since the Second Circuit had not decided a data breach case yet.[62]

After surveying the principles of Article III standing and the circuit split, the court analyzed the imminence of identity theft based on *Clapper.* It concluded the alleged future injury

was not certainly impending. The court relied on findings from an investigation initiated by Excellus after the breach. According to the court, the investigation produced insufficient evidence to show the hackers intended to use the information for identity fraud.[63] Echoing *Clapper*, the court defined a chain of events that would have to occur in order for the "non-misuse plaintiffs" to experience identity theft. Such attenuation, in combination with the time transpired since the breach, led the court to conclude identity theft was not certainly impending and therefore not an injury in fact.[64] The court's decision runs counter to precedent cited from the Sixth, Seventh, and Ninth Circuits, but agrees with the Third and Fourth Circuits and several district courts which also denied standing to data breach victims.[65]

III. ANALYSIS

Excellus presented an opportunity for the district court to conduct a thorough analysis ahead of the court of appeals taking a position in the circuit split. Now that the opinion from *Whalen v. Michaels Stores* was issued but is not precedential,[66] the incoherent opinion the district court delivered is particularly regrettable because the court of appeals position is unreliable too. This Comment critiques the court's approach from analytical and policy perspectives, and in light of the subsequent *CareFirst* decision from the D.C. Circuit Court of Appeals.

A. The Standard of Review Is Inconsistent with Precedent and Prejudices Plaintiffs

The court relied on Second Circuit precedent to set the standard of review and burden of proof for the 12(b)(1) motion to dismiss for lack of subject matter jurisdiction. It required the plaintiffs to prove each element of standing by a preponderance of the evidence and permits the court to refer to evidence outside the pleadings.[67] This standard is conflict with rules from the Supreme Court on motions to dismiss and contrasts with other data breach cases.[68] Imposing a preponderance of the evidence standard prejudices plaintiffs who have no way of knowing the

likelihood of identity theft.[69] If the court followed the Supreme Court's standard, it could have inferred the sixteen allegations of misuse, in combination with the fact the investigation "was unable to rule out the possibility the attacker accessed patient data based on the available log data"[70] indicated the data was accessed with intent to commit fraud. Admittedly, lenient pleading requirements for standing could formalistically threaten the separation of powers.[71] However, the Supreme Court implicitly rejected that notion when it let *CareFirst* stand, as the D.C. Circuit analyzed standing at the pleadings with a plausibility standard.[72] The plausibility approach is appropriate from a policy perspective because, at the pleading stage, the "benefit of the doubt . . . should be given to the party with the least information."[73]

B. The Court Failed to Clearly Articulate its Rule for Data Breach Injury in Fact

This case was an opportunity for the court to stake its position on how to properly analyze standing in data breach cases, but its rule discussion and analysis are disjointed. The court analogized to *Clapper*[74] but did not explain why it rejected other noted approaches, unlike other courts that have faced the issue.[75] For example, the court cited the framework in *Khan v. Children's Nat'l Health Systems* for standing via either "actual examples of the use of the fruits of the data breach for identity theft, *even if involving other victims*; or a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud."[76] Yet the court ignored the fact there were allegations of fraud against other victims.[77] This contradiction without explanation undermines the opinion's precedential value because both the rule employed and the facts taken as pertinent are unclear.

The analysis is also incomplete. The court only considered standing for future injuries if they are "certainly impending" despite noting the applicability of the "substantial risk" standard.[78] It is possible the court viewed these standards as requiring the same type of risk.[79]

However, if "substantial risk" does require something different than "certainly impending," the analysis denied the plaintiffs full consideration. Furthermore, the court did not consider the possible influence of the type of data exposed, even though healthcare data breaches are considered among the most serious.[80] The *CareFirst* court relied heavily on the type of data in its decision to find standing, and the data there was very similar to *Excellus*.[81] With the benefit of hindsight, this fact may have been relevant.

C. The Outcome Creates an Arbitrary Standard for Redress and Liability

The holding in *Excellus* effectively permits claims to go forward if exposed data was misused but stymies claims if not. This rule is rooted in the actions of third parties rather than focused on what a defendant did or did not do, despite the court's façade that the claims are dismissed to avoid just that.[82] One can imagine how this metric would play out in future data breaches: even if a business took reasonable precautions and followed disclosure rules, it could be forced to settle a lawsuit because consumer data was misused. On the contrary, a business that was negligent in providing data security could be off the hook if the stolen data was not misused. If the goal of data breach litigation is to improve data security and prevent breaches,[83] this rule does not work because liability is based partially on chance, providing few incentives to be proactive.

If this precedent is followed, consumers would wrongly be denied the ability to seek protection before harm comes to them, a right recognized by the Supreme Court. [84] Just as accountability will be based on the actions of third parties, so too will the ability of plaintiffs to seek redress, resulting in greater uncertainty.[85] Particularly in the health care context, consumers have little agency to change providers or to change their personal information.[86] Risk averse and prudent consumers will likely still take precautions after a data breach.[87] Even if a company was

negligent, consumers could be stuck with mitigation costs and the risk of future fraud without redress because their data was not misused by the hackers, meaning there is no standing.[88]

This outcome may be defensible from a formalist perspective that places great emphasis on following standing doctrine to ensure the separation of powers and avoid the court stepping outside the case or controversy prerequisite.[89] But the plaintiffs in data breach litigation have a personal stake in the matter because it was their personal information that was compromised. According to *CareFirst*, ensuring parties have a personal stake in litigation is the core of standing doctrine.[90]

D. *Excellus* Illustrates the Usefulness of a Uniform Rule

The perverse outcomes of this case—that it perpetuates what the court purports to avoid—illustrate how the existing legal options leave consumers caught up between "a justice-based desire for rectifying or preventing damages, and a legal requirement that damages be articulable in terms that data breaches defy."[91] Likewise, businesses are faced with uncertainty about their potential liability after the unfortunate event of a data breach. Resolution of this tension and uncertainty requires a uniform rule regarding data breach harm set by the Supreme Court or Congress.[92] Legislative action would provide an opportunity to address national security and international relations concerns regarding data security, something outside the Court's reach.[93]

A statute or a Supreme Court ruling could pave the way for fairer adjudication focused on causation and liability of businesses rather than injury in fact based on happenstance. Detailed discussion about the content of a future rule is outside the scope of this Comment. However, for consideration, an efficacious rule could, for example, recognize risk of identity theft as a categorical injury.[94] It might accept reasonable mitigation efforts or anxiety about identity theft

as injury in fact.[95] The Court could announce an adjusted standing framework, since data breach litigation typically lacks the constitutional and foreign affairs dimensions of *Clapper v. Amnesty International, USA.*[96] No matter which takes hold, data breaches will likely continue and lawsuits will inevitably follow, meaning standing will continue to be an issue for federal courts.

CONCLUSION

A subset of plaintiffs in the class action data breach lawsuit *Fero v. Excellus Health Plan, Inc.* alleged injury based on increased risk of future identity theft without their own compromised personal information being misused. The court isolated these plaintiffs from the others and dismissed their claims because the alleged increased risk was not certainly impending, and therefore not sufficient for injury in fact under the standing requirements of *Clapper.* The court permitted other plaintiffs who did allege misuse to proceed in litigation. Deciding standing based on misuse relies on the conduct of third parties. Consumers and businesses are therefore subject to arbitrary redress and liability. Between this effect and the court's tenuous analysis, *Excellus* is an excellent illustration of why data breach litigation needs a new, uniform rule. In order to improve data security and create fairer outcomes, future legislation or Supreme Court rulings should focus on determining liability for attacks rather than injury to consumers.

---

[1] Fero v. Excellus Health Plan, Inc., 236 F. Supp. 2d 735, 744 (W.D.N.Y. 2017) (outlining the events during and after the data breach).

[2] *Id.* at 743–45 (describing the parties, claims, and procedural posture).

[3] *Id.* at 753 (holding alleged injuries to be speculative rather than certainly impending).

[4] *See, e.g.*, In re SuperValu, Inc., 870 F.3d 763, 769 (8th Cir. 2017) (refusing to reconcile the circuit split because differences can be explained by facts).

[5] *Compare* Remijas v. Neiman Marcus Group, LLC., 794 F.3d 688, 694 (7th Cir. 2015) (inferring substantial risk based in part on Neiman Marcus's offer of credit monitoring), *with* Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017) (declining to infer substantial risk).

[6] Attias v. CareFirst, Inc., 865 F.3d 620, 625 (D.C. Cir. 2017).

[7] *Cf.* Brief of Amicus Curiae Electronic Privacy Information Center in Support of Plaintiffs-Appellants/Cross-Appellees at 27, In re Supervalu, Inc., 870 F.3d 763 (8th Cir. 2017) (Nos. 16-2378, 16-2528) [hereinafter EPIC] (explaining importance of litigation to increase data security).

[8] *Excellus*, 236 F. Supp. 2d at 749.

[9] *See Genesis* 27:35–45 (King James) (describing the blessing lost by Esau); WILLIAM SHAKESPEARE, OTHELLO act 3, sc. 3 ("[H]e that filches from me my good name . . . makes me poor indeed.").

[10] *Cf.* 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 (observing it is "awkward" to apply existing legal theories to data breaches).

[11] Adam Shell, *Equifax Data Breach Could Create Lifelong Identity Theft Threat*, USA TODAY (Sept. 9, 2017, 7:00 AM), https://www.usatoday.com/story/money/2017/09/09/Equifax-data-breach-could-create-life-long-identity-theft-threat/646765001.

[12] *See, e.g.*, Eric Cernak, *Why Data Theft Poses a Big Risk to Small Businesses*, USA TODAY: CYBERTRUTH (May 6, 2013, 12:48 PM), https://www.usatoday.com/story/cybertruth/2013/05/06/data-breach-small-business-cybersecutiry-online-privacy/2138713/ (dispelling myth data breaches only impact big business); *Officials Say Residents' Data Possibly Hacked in Data Breach* (Fox 5 Atlanta television

broadcast Mar. 27, 2018), https://www.youtube.com/watch?v=TVkJZwEjdh8 (discussing data breach of local government).

[13] PONEMON INSTITUTE, 2013 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS, 6 fig.4 (2013); Vincent Liu, Mark A. Musen & Timothy Chou, Research Letter, *Data Breaches of Protected Health Information in the United States*, 313 J. AM. MED. ASS'N 1471, 1471 (2015).

[14] *See, e.g.*, Amanda Bronstad, *Regulators, Not Class Actions, Could Drive Legal Response to Uber Data Breach*, THE 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/ (noting a dozen class action lawsuits were filed within a week of the Uber data breach being announced). *But see* Seena Gressin, *The Equifax Data Breach: What to Do*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, (Sept. 8, 2017), https://consumer.ftc.gov/blog/2017/09/equifax-breach-what-do (recommending various ways other than filing a lawsuit to protect one's self after a data breach).

[15] *Compare* Edward Pettersson, *Equifax May Be Happy Paying $1 per Customer for Their Hassle*, BLOOMBERG (Sept. 20, 2017, 5:14 PM), https://www.bloomberg.com/news/articles/2017-09-20/Equifax-may-be-happy-to-spend1--per-customer-for-their-trouble ("[A] lot of defendants welcome these lawsuits . . . ."), *and* Reuters, *Target Settles 2013 Hacked Customer Data Breach for $18.5 Million*, NBC NEWS: BUS. (May 24, 2017, 10:49 AM) (noting Target keeps funds on reserve for data breach settlements), *with* Brief of the Chamber of Commerce of the United States of American as Amicus Curiae in Support of Appellees, Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017) (No. 16-7108), 2017 WL 632533 [hereinafter Chamber of Commerce] ("[L]awsuits . . . threaten to extract massive settlements from businesses that were victimized by hackers or thieves."), *and* Petition

for Rehearing En Banc, Remijas v. Neiman Marcus Group, LLC., 794 F.3d 688 (7th Cir. 2015) (No. 14-3122), 2015 WL 4639951 (fighting the lawsuit because credit monitoring is merely "routine behavior necessary in the modern age of widespread credit card use.").

[16] Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Cases*, WALL STREET J. (June 26, 2016, 8:06 PM), https://wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988 ("The main early issue in [data breach] lawsuits is whether customers can show that a data breach injured them personally . . . .").

[17] U.S. CONST. art. III, §§ 1–3.

[18]Attias v. CareFirst, Inc., 865 F.3d 620, 625 (D.C. Cir. 2017) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)). *But see Standing*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining standing in terms other than the three elements).

[19] *See generally* THE FEDERALIST NO. 78 (Alexander Hamilton) (describing limits on judiciary).

[20] BLACK'S LAW DICTIONARY, *supra* note 18 ("The word standing is rather recent. . . .").

[21] Daniel R. Stoller, *SuperValu Data Breach Claim Nixed, Court Sees No Consumer Harm*, BLOOMBERG L.: PRIV. & DATA SECURITY (Mar. 8, 2018), https://www.bna.com/supervalu-data-breach-n57982089668/ ("[C]onsumers have struggled to succeed in data breach class actions, and the stumbling block has been an inability to show . . . imminent and direct harm.").

[22] *E.g.*, Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 745–46 (W.D.N.Y. 2017)

[23] *E.g.*, In re SuperValu, Inc., 870 F.3d 763, 771 (8th Cir. 2017) ("Because plaintiffs have not alleged a substantial risk . . . the time they spent protecting themselves against this speculative threat cannot create an injury.").

[24] Clapper v. Amnesty International USA, 568 U.S. 398, 409 (2013); *Id.* at 441 n.5.

[25] *Id.* at 422 (holding that respondents lack Article III standing).

[26] *See Id.* at 408–09 (reviewing prior cases where the standing inquiry was especially rigorous).

[27] 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 CREIGHTON L. REV. 467, 487 (2016) ("[W]hat satisfies the injury-in-fact requirement of standing . . . is unsettled."); *see also* Beck v. McDonald, 848 F.3d 262, 272 (4th Cir. 2017) (rejecting the contention that *Clapper* imposes a heightened burden). Jordan Z. Dillon, Comment, *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, 143–44 (2017) (chastising the Seventh Circuit for an incorrect interpretation of *Clapper*).

[28] *See, e.g.*, In re Supervalu, Inc., 870 F.3d 763, 769 (8th Cir. 2017) (refusing to reconcile the circuit split because differences can be explained in difference in substance of the allegations).

[29] Martin H. Redish & Sopan Joshi, *Litigating Article III Standing: A Proposed Solution to the Serious (But Unrecognized) Separation of Powers Problem*, 162 PA. L. REV. 1373, 1376–77 (2014) (comparing standards of review for 12(b)(1)).

[30] Attias v. CareFirst, Inc., 865 F.3d 620, 626–27 (D.C. Cir. 2017) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

[31] *See, e.g.*, *In re SuperValu*, 870 F.3d at 768 (stating the court will draw all inferences in the plaintiffs' favor when deciding the motion to dismiss because the defendants attack standing).

[32] *Compare* Galaria v. Nationwide Mutual Insurance, Co., 663 Fed. Appx. 384, 388 (6th Cir. 2016) (drawing an inference that if a breach targets information there will be fraud), *with* Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 752–51 (W.D.N.Y. 2017) (discussing *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524 (D. Md. 2016) wherein the court declined to infer the purpose of data theft).

[33] *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017) (reversing because of allegations that social security numbers were exposed in the breach).

[34] *E.g.*, *Galaria*, 663 Fed. Appx. at 389 (discussing the impact of whether there was an intentional theft on standing in different circuit court precedent).

[35] 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 ("[I]t is likely the Supreme Court will take up the case.").

[36] CareFirst, Inc. v. Attias, 138 S. Ct. 981 (2018) (denying petition for writ of certiorari).

[37] *CareFirst*, 865 F.3d at 629.

[38] *Id.* at 628.

[39] 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/.

[40] *Compare* CAL. CIV. § 1798.82 (2018) (requiring notification to consumers after data breaches), *with* COLO. REV. STAT. § 6-1-713 (providing guidelines for destruction and preservation of consumer information), *and* 201 MASS. CODE REGS. 17.00 (2010) (setting "minimum standards to be met in connection with the safeguarding of personal information . . . .").

[41] John Biglow, Note, *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, 959 (2016). *Contra* Sasha Romanosky, Rahul Telang & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL. ANALYSIS & MGMT. 256, 281 (2011); Ravi Sen & Sharad Borole, *Estimating the Contextual Risk of Data Breach: An Empirical Approach*, 32 J. MGMT. INFO. SYS. 314, 320 (2015) (proposing disclosure laws work based on criminology and empirics).

[42] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 781 (2018).

[43] Cernak, *supra* note 12 (stating that some small businesses neither know of, nor follow laws).

[44] *See* Benjamin Schwartz, THE NEW YORKER: DAILY CARTOON (Sept. 23, 2016), https://www.newyorker.com/cartoon/daily-dartoon-092316-yahoo (making light of delay in disclosure).

[45] PONEMON INSTITUTE, *supra* note 13, at 9, fig.9.

[46] *See generally* Julie Brill, Comm'r, Fed. Trade Comm'n, Back to the Future: Meeting Privacy Challenges Through a Strong Transatlantic Relationship, at 5–6, (Dec. 10, 2015) 2015 WL 9684102 (F.T.C.) (describing existing mechanisms to protect data at federal level); *see also* Privacy Act of 1974, 5 U.S.C. § 552a (2016) (requiring only federal agencies to establish appropriate safeguards for recordkeeping); Video Privacy Protection Act, 18 U.S.C. § 2710 (2013) (prohibiting disclosure of personally identifiable information).

[47] *Compare* Kim Zetter, *National Data Breach Laws Move Through Senate*, WIRED (Nov. 6, 2009, 5:29 PM), https://www.wired.com/2009/11/breach-laws/ (noting legislative progress in 2009), *with* Bronstad, *supra* note 14 (speculating about legislation again in 2018).

[48] Personal Data and Security Act, S. 1490, 111th Cong. § 2(4) (2009) (recognizing the seriousness and need to prevent identity theft).

[49] *Compare,* Chamber of Commerce, *supra* note 15 (describing business interests), *with* EPIC, *supra* note 7 (describing consumer interests).

[50] *Compare* Chamber of Commerce, *supra* note 15, at 25 ("[M]otivation for avoiding data breaches surely comes from the substantial public relations harm . . . ."), *with* Patrick J. Lorio,

Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79 (2017) (advocating for a statute).

[51] *E.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (denying standing for intangible injury even though there was a statute in place that created a cause of action). *But cf.* Lorio, *supra* note 50, at 117–20 (describing careful legislation that could confer standing to data breach victims).

[52] Google, Inc., No. C-4336 2011 WL 5089551 (F.T.C.) (2011), at 9–12 (resulting in orders for actions going forward, but no orders regarding remedies for consumers); Biglow, *supra* note 40, at 960 ("the FTC cannot issue civil penalties . . . "); Matsakis, *supra* note 39 (quoting the view that federal legislation would "water down" current state level requirements).

[53] Ifrah PLLC, *The Data Breach Legal Limbo on Consumers' Ability to Sue Hacked Companies*, IFRAH L.: FTC BEAT (January 16, 2018), https://jdsupra.com/legalnews/the-data-breach-legal-limbo-on-62346/ ("the trend is toward responsible data stewardship. . . ."); *see also* Mark Zuckerberg, FACEBOOK, (Mar. 21, 2018, 2:36 PM), https://www.facebook.com/zuck/posts/10104712037900071 (announcing a company-wide plan to improve data security and privacy without coercion from legislation or litigation).

[54] *See* Personal Data and Security Act, *supra* note 48, at § 2(2) ("[I]dentity theft is a serious threat to the Nation's economic stability, homeland security, the development of e-commerce."); S.M. Furnell & M.J. Warren *Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?*, 18 COMPUTERS & SECURITY 28 (1999) (discussing risks of cyberterrorism).

[55] *See* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650, ¶ 108 (holding that Safe Harbor principles no longer protect United States companies from data security challenges). *See generally* Data Privacy Act of 2012, Rep. Act No. 10173, §§ 11–20 (Aug. 5, 2012) (Phil.) (illustrating comprehensive data privacy legislation); *Data Privacy, Ethics and Protection:*

Guidance Note on Big Data for Achievement of the 2030 Agenda, U.N. DEV. GRP. (2015) (suggesting international standards for data security).

[56] *See* Lorio, *supra* note 50, at 118 ("The relevant question for policymakers must be which parties are best able to bear the risk . . . . [I]t would be nearly impossible for individuals to participate in the modern economy without sharing personal information on a near-daily basis.").

[57] *See* Baer & Sharma, *supra* note 10 (observing that the theory of future harm is most applicable to data breaches "but it is in conflict with the requirements of standing . . . .").

[58] Lorio, *supra* note 50, at 117 (describing potential benefits to businesses from a statute).

[59] Fero v. Excellus Health Plan, Inc., 236 F. Supp. 2d. 735, 745 (W.D.N.Y. 2017).

[60] *Id.* (listing ten causes of action including breach of contract and statutory violations).

[61] *Id.* at 746 (stating the standard of review for a motion to dismiss under Rule 12(b)(1)).

[62] *Id.* at 749 (surveying the circuit split and noting the Second Circuit is about to join a side).

[63] *Id.* at 753 (explaining the implications of the investigation for standing).

[64] *Id.* ("[A]lleged injuries are neither concrete nor actual and imminent because [they] rely on a chain of possibilities about the actions of independent actors.").

[65] *Excellus*, 236 F. Supp. 2d. at 749.

[66] Whalen v. Michaels Stores, Inc., 689 Fed. Appx. 89 (2d Cir. 2017); 2D CIR. R. 32.1.1.

[67] *Excellus*, 236 F. Supp. 3d at 746 (quoting Makarova v. United States, 201 F.3d 110, 113 (2d Cir. 2000)).

[68] *See e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620, 625 (D.C. Cir. 2017) (requiring that each standing element is represented by a plausible claim in the pleadings).

[69] *Cf.* Biglow, *supra* note 41, at 967 (arguing plaintiffs should not have to plead with particularity when the defendants have all the information about the breach).

[70] *Excellus*, 236 F. Supp. 3d at 753.

[71] *See* Redish & Joshi, *supra* note 27, at 1399 (arguing that a low burden for standing at the pleading stage "allows courts to stay beyond their constitutionally permissible role . . . .").

[72] *CareFirst*, 865 F.3d at 625.

[73] Biglow, *supra* note 40, at 967. *Contra* Redish & Joshi, *supra* note 29, at 1377 ("[C]ourts should address all factual issues relevant to standing by conducting limited discovery . . . .").

[74] *Compare Excellus*, 236 F. Supp. 3d at 753 (concluding the alleged injuries "rely on a chain of possibilities") *with* Clapper v. Amnesty International, USA, 568 U.S. 398, 414 (2013) ("[R]espondents' speculative chain of possibilities does not establish the injury . . . is certainly impending . . . .").

[75] *E.g.*, In re SuperValu, Inc. at 769 (explaining why it does not reconcile the circuit split).

[76] *Excellus*, 236 F. Supp. 3d at 753 (quoting *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 531 (D. Md. 2016)).

[77] *Id.* at 786 (denying non-misuse claims but proceeding with misuse claims).

[78] *Id.* at 749; *see also* In re Supervalu 870 F.3d 763, n.3 (8th Cir. 2017).

[79] *See* Wilka, *supra* note 27, at 488 (acknowledging the difference between standards is unclear).

[80] *Id.* at 484–85 (stating medical identity theft victims suffer more harm than credit card fraud).

[81] *Attias v. CareFirst, Inc.*, 865 F.3d at 627–28.

[82] *Excellus*, 236 F. Supp. 3d at 753.

[83] *E.g.*, Baer & Sharma, *supra* note 10 (listing purposes of litigation, including compensation and avoiding data breaches in the future).

[84] *See* In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) (explaining the "well-established principle" that injury in fact does not have to be certain).

[85] *Contra* 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 (speculating that recent court decisions increase the certainty of standing and redress in court).

[86] Solove & Citron, *supra* note 42, at 758 (noting social security numbers and health information cannot be or are very difficult to change).

[87] *See* Galaria v. Nationwide Mutual Insurance Co., 663 Fed. Appx. 384, 88 (6th Cir. 2016) (indicating that "where plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse" to take precautions).

[88] Solove & Citron, *supra* note 42, at 758 ("[C]onsumers bear the lion's share of [opportunity] costs because courts view them as too attenuated to recognize as harm."). *Cf. id.* at 757–58 (proposing the involvement of third parties makes breaches harmful and impedes litigation).

[89] *See generally* Redish & Joshi, *supra* note 29 (arguing *Lujan* standard violates judicial power).

[90] Attias v. CareFirst, Inc., 865 F.3d 620, 626 (D.C. Cir. 2017).

[91] Baer & Sharma, *supra* note 10.

[92] *See* Lorio, *supra* note 50, at 118 (describing current uncertainty faced by businesses).

[93] Clapper v. Amnesty International USA, 568 U.S. 398, 408–09 (2013).

[94] *See* Solove & Citron, *supra* note 43, at 777 ("Instead of certainties, we need to shift the focus to risk because contemporary understandings of the world are based on risk.").

[95] *See* Megan Dowty, Note, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 713 (2017) ("Money spent on monitoring services results in a concrete, particularized, and redressable injury, and it should be compensated . . .").

[96] Wilka, *supra* note 27, at 481–84 (arguing for a lower standing threshold in data breach cases).