Note

Data Breach Class Actions: How Article III Standing Analysis Should Evolve After *TransUnion, LLC v. Ramirez*

Caleb A. Johnson∗

In early November 2021, nearly 7 million Robinhood users woke up to a message no one wants to see: Robinhood had been hacked.[1] Users did not need to worry of what financial ruin might lie ahead, as Robinhood quickly announced that the hack compromised "only" five million emails, two million full names, and several thousand phone numbers.[2] The data security incident at Robinhood was not as catastrophic as it could have been, but it raises a question. What could users do if Robinhood actually lost their more sensitive personal and financial information, like their social security numbers or bank accounts, to hackers?

Hacks and data breaches have become a staple in the American vernacular.[3] This is not just because of all the movies showing self-proclaimed geeks breaking into computers, but because the risk of losing personal data is an almost foregone conclusion to younger generations.[4] Data breaches are frequently in the news, and companies even offer rewards to the public for helping

∗ J.D. Candidate, Minnesota Law School 2023; Managing Editor, *Minnesota Law Review*, Vol. 107. My heartfelt thanks to Professor Alan Rozenshtein and the students at *Minnesota Law Review* for their thoughtful feedback while I developed this Note. Special shout-out to my wife Anneke for letting me work on this Note during many times in our life together when it would have been much easier if I wasn't working.

1. *Robinhood Announces Data Security Incident (Update)*, ROBINHOOD (Nov. 16, 2021), https://blog.robinhood.com/news/2021/11/8/data-security-incident [https://perma.cc/U8HJ-AHPR].

2. *Id.*

3. *E.g.*, Chris Velazco, *Hacks and Data Breaches Are All Too Common. Here's What to Do If You're Affected.*, WASH. POST (Oct. 14, 2021), https://www.washingtonpost.com/technology/2021/10/14/hacked-what-to-do [https://perma.cc/K3DD-KQNB] ("Hacks and data breaches have become a persistent part of life in the 21st century, and the proof is in the news.").

4. *Id.*

prevent them.[5] In 2021, 1,862 data compromises were publicly reported, impacting over two trillion victims—the largest number of compromises ever recorded in a calendar year.[6]

Some consumers have used lawsuits as a remedy for these data breaches.[7] Most disputed data breach claims in federal courts are not actually between the hacker and the individuals with compromised data.[8] Rather, since companies and consumers may be unable to identify the hacker, and companies tend to have more money accessible to plaintiffs than criminals, consumers file claims against the company that lost the data.[9] For many of these claims, plaintiffs face difficulty proving that they have Article III standing to bring suit against the

---

5. Davey Winder, *Microsoft Paid Hackers More Than $13 Million in Past 12 Months*, FORBES (Aug. 5, 2020), https://www.forbes.com/sites/daveywinder/2020/08/05/microsoft-paid-hackers-more-than-13-million-in-past-12-months-windows-xbox-edge-azure [https://perma.cc/4PM5-RJBW] (describing how Microsoft paid millions of dollars through a bounty program where the company incentivized hackers to look for issues in Microsoft code and report the bugs to Microsoft so the bugs can be fixed rather than the hackers exploiting the issues for personal gain).

6. This includes over 189 million U.S. victims of data breaches, over 104 million U.S victims of data exposures, and 1.8 trillion U.S. and non-U.S. victims of data leaks. *2021 in Review: Data Breach Annual Report*, IDENTITY THEFT RES. CTR. 6–7 (2022) [hereinafter ITRC REPORT 2021], https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2 [https://perma.cc/9RKQ-XEQM]; s*ee Robinhood Headlines November Data Breaches; Number of Compromises Reaches All-Time High*, IDENTITY THEFT RES. CTR. (2021), https://us19.campaign-archive.com/?u=fba66e1a225eda5e30bd00da9&id=6d4266a247 [https://perma.cc/69Y2-CRXH] ("The Identity Theft Resource Center (ITRC) has been tracking publicly-reported data breaches and exposures since 2005. Over the last 15 years, the high-water mark for breaches was in 2017 with 1,529 data compromises."); *see also* Chris Morris, *The Number of Data Breaches in 2021 Has Already Surpassed Last Year's Total*, FORTUNE (Oct. 6, 2021), https://fortune.com/2021/10/06/data-breach-2021-2020-total-hacks [https://perma.cc/6MMH-FLZC] (referencing the work of the ITRC). The Identity Theft Resource Center focuses on reporting information if at least one state data breach notice law protects a piece of information. ITRC REPORT 2021, *supra*, at 29.

7. *See, e.g.*, Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1325–26 (2017) (describing how plaintiffs allege that the company inadequately protected their personal information and that justifies the suit).

8. *Id.*

9. *Id.*

company.[10] This difficulty is because plaintiffs don't always wait to sue until after the hacker starts fraudulently using their information.[11] They sue based on their already exposed information and want the company to help pay to prevent potential fraud.[12]

Article III standing doctrine is based in separation of powers principles that federal courts should have limited jurisdiction.[13] The constitutional doctrine has grown out of the idea that judicial action must stem from a case or controversy.[14] The factors used in the analysis of finding Article III standing are of judicial creation and are the first barrier to a suit going forward in federal court.[15] Over time, this doctrine remains unclear, and there is room for improvement in clarifying the path to standing. The Supreme Court has stressed the importance of having an "injury-in-fact" to have Article III standing, and circuit courts have various ways of deciding whether or not a data breach victim has sufficient injury-in-fact before their information has been misused.[16]

This Note will summarize Article III standing in data breach litigation with a focus on the important changes from 2021 and argue that a brighter rule would be more efficient and is needed to bring clarity to consumers and companies alike. Part I gives an overview of data breaches and class actions. Part II explains general Article III standing, including a summary of the 2021 Supreme Court case *TransUnion, LLC v. Ramirez*.[17] Part III summarizes the current state of federal appellate data breach cases. Part IV analyzes data breach caselaw after *Ramirez* with an eye towards the distinctions provided in Part I and II. Part V provides an overview of this Note's proposed rule for data breach standing. The proposition is that standing under the substantial risk of harm theory should be entirely based on the type of data lost in the breach. Part VI applies the proposed rule to the circuit cases discussed in Part II and calls for the Government

10. *See infra* Part II; Marcello Antonucci, Jana Landon, Chad Layton & Darin McMullen, *Article III Standing in Cyber-Breach Litigation*, BRIEF, Summer 2019, at 36, 38.

11. *Id.*

12. *Id.*

13. *See infra* Part II.B; U.S. CONST. art. III, § 2.

14. Spokeo, Inc. v. Robins, 578 U.S. 330, 337–38 (2016).

15. Antonucci et al., *supra* note 10.

16. *Id.*

17. 141 S. Ct. 2190 (2021).

Accountability Office to provide an updated report on the impact of data breaches and identity theft by evaluating incidents more recent than those from 2005.

I. WHAT ARE DATA BREACHES AND WHAT ARE THEY DOING IN COURT?

When a company has experienced a data breach, it does not automatically mean that a court case will ever be filed. Sometimes the breach turns out to not actually have included sensitive consumer data. Other times the company helps protect the breached consumer data so completely that most consumers do not file suit. The other times lead to a much higher potential for court involvement, when sensitive data is compromised, and the company does not support its consumers. This section will give an overview of what constitutes a data breach, and how such incidents come about.

A. BACKGROUND ON DATA BREACHES

This Note will strive to follow the definitions used by the Identity Theft Resource Center (ITRC) as an aggregated way to account for the differences between various state codes.[18] The ITRC is a national non-profit that provides advice and assistance to victims of identity crime, and maintains the largest repository of U.S. data breach information.[19] The definitions introduced here are important for following the otherwise very similar cases under the overarching term "data breach litigation."

1. Data Breaches Are Growing More Common, But Defining Terms Is Becoming More Difficult

Consumers give companies their data for any number of reasons: ease of not having to remember their account info,[20] wanting a more personalized experience,[21] or unknowingly.[22] Allowing a company to have access to your personal information can

18. *2020 in Review: Data Breach Report*, IDENTITY THEFT RES. CTR. 27 (2021) [hereinafter ITRC REPORT 2020], https://notified.idtheftcenter.org/s/2020-data-breach-report [https://perma.cc/9PDM-ENP6].

19. *About Us*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/about-us [https://perma.cc/AE6D-6UF5].

20. Going back to a website that has remembered your log in password and your credit card info for checkout, for example.

21. Allowing tracking for personalized ad experience, like Facebook or YouTube.

22. *See, e.g.*, Caroline Cakebread, *You're Not Alone, No One Reads Terms of*

be very convenient. For example, giving online retailer Zappos! your name, credit card number, and home address allows for shoes to be delivered to your front door. Another example, giving Apple or Samsung your fingerprint allows for easier opening of a locked phone. The issues arise when a consumer's personal data held onto by the company is compromised.

Data compromise is an umbrella term used to encompass data breaches, data exposures, and data leaks.[23] Data exposure describes when personally identifiable information (PII) is not secured, but there is not yet evidence of removal or misuse.[24] Data leaks consist of PII that has become publicly available, and the PII is low risk when viewed individually, but at sheer volume the leaks create a risk of social engineering.[25] Data breaches are what you would expect, hackers get data.[26] Data compromises, mostly breaches, lead to consumer PII being available to unintended parties.[27] This information can be used by bad actors to log in to people's accounts, place unauthorized charges on credit cards, and depending on the sensitivity of the information it can be used to open new accounts.[28]

An authoritative definition of PII used in multiple circuit opinions, and by many parties in their complaints, comes from a Government Accountability Office (GAO) report.[29] In 2007, the GAO defined PII as anything "to distinguish or trace an individual's identity—such as name, Social Security number, driver's license number, and mother's maiden name—because such information generally may be used to establish new accounts, but

---

Service Agreements, BUS. INSIDER (Nov. 15, 2017), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/SR7S-WW75] (referencing a Deloitte survey of 2,000 consumers that found over ninety percent accept legal terms and conditions without reading them).

23. ITRC REPORT 2021, *supra* note 6, at 28.

24. *Id.* For example, if it's reported that there's a vulnerability in a company's database but no proof that a hacker actually exploited the weakness, then it's an exposure.

25. Social engineering is "where savvy cybercriminals trick[] people into revealing information needed to launch an attack." *Id.* at 3–4.

26. *Id.* at 28.

27. *Id.*

28. *Id.*

29. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015); *In re* Zappos.com, Inc., 888 F.3d 1020, 1024 n.3 (9th Cir. 2018); *In re* SuperValu, Inc., 870 F.3d 763, 766–67 (8th Cir. 2017); Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1342–43 (11th Cir. 2021); Legg v. Leaders Life Ins. Co., 574 F.Supp.3d. 985, 991 (W.D. Okla. 2021).

not to refer to other 'means of identification,' . . . such as credit or debit card numbers."[30] This report analyzed data breaches that took place from 2000 to 2005 and gave a summary on the impacts of identity theft on Americans and next steps.[31] However, the report ends giving no recommendations and not conclusively leaning one way or another on risk levels of identity theft from breaches.[32] The 2007 GAO Report is not the most recent attempt to define PII, but it is worth noting the recent references and weight given to the GAO report in 2021 cases despite the report's age. The age of the report is a fact not lost on the courts.[33]

Interestingly, in 2008, the GAO redefined PII to also include "any other information that is linked to an individual."[34] The 2008 GAO report expanded the scope of PII to include the "other means of identification"[35] that the 2007 report had excluded from its definition: the information that could be used to fraudulently use financial accounts, but not sensitive enough to open new accounts.[36] This GAO shift shows that the ideas around the definition of PII are a balancing act between trying to show the significant, sensitive nature of some information while also allowing for PII to be an umbrella that covers the more literal and broad definition of personal information.

This Note will distinguish PII into two categories: static and dynamic. Static PII is information that is not easily changed by an individual and can be used to open new accounts, such as full name, date of birth, social security number, and biometric data. Dynamic PII is information that could be changed without extreme difficulty and cannot be used to open new accounts, such as credit card number, debit card PIN, and account password.

---

30. U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 2 n.2 (2007) [hereinafter GAO REPORT 2007].

31. *Id.* at 5–7.

32. *Id.* at 7.

33. *Tsao*, 986 F.3d at 1343 ("Of course, we recognize that the GAO Report is over a decade old . . . .").

34. U.S. GOV'T ACCOUNTABILITY OFF., GAO-08-536, PRIVACY: ALTERNATIVES EXIST FOR ENHANCING PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION 1 n.1 (2008) [hereinafter GAO REPORT 2008].

35. GAO REPORT 2007, *supra* note 30 (internal quotation omitted).

36. *Compare* GAO REPORT 2008, *supra* note 34*, with* GAO REPORT 2007, *supra* note 30.

The court cases that will be discussed did not originally use 'dynamic' and 'static,' but for clarity this Note categorizes the cases using these definitions.

Data breaches can be a highly stressful event for companies.[37] In the heat of the tense moments after a hacker breaches a company's defenses, companies may feel like keeping the embarrassment to themselves rather than sharing with the world. Through state data breach notification laws, the government has decided that companies are not entitled to keep data breaches of consumer PII quiet.[38]

2. Notification Laws Differ in Definitions but Not in Intention

When a company realizes there has been a data breach, various state laws require that if consumer data is compromised, the consumer must be notified.[39] The main goals of these laws are (1) to incentivize improved institutional data security (companies want to avoid the embarrassment of publicly admitting security breaches) and (2) to create informed consumers.[40] Consumers can take appropriate action only if they know there's an issue with their data.

A downside to the state-by-state approach of notification laws is that every state has created a slightly different definition for what personal information must be reported. For example, Minnesota requires notification for "personal information" defined to include an individual's name in combination with either a Social Security number (SSN), driver's license number, or financial account number in combination with the passcode that permits access to the account.[41] California's law defines personal information to include all of the information in Minnesota's definition, but also includes medical information, biometric data, genetic data, and email password combinations.[42] Texas requires

37. Tommy Johnson, *The Impact of a Data Breach*, SECURITY MAG. (Sept. 13, 2022), https://www.securitymagazine.com/articles/98325-the-impact-of-a-data-breach [https://perma.cc/B2M7-PBGR].

38. *See, e.g.*, William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1152 (2019).

39. *See id.*; *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Nov. 24, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/QM8Y-6DUU].

40. McGeveran, *supra* note 38.

41. MINN. STAT. ANN. § 325E.61(e) (West 2023).

42. CAL. CIV. CODE. § 1798.82(h) (West 2022).

breach notification for "sensitive personal information," which includes the information in Minnesota's definition plus information related to physical and mental health as well as healthcare.[43] These are three anecdotal examples to show that although many states have similar desires to protect citizens' information, states disagree on the types of data that should be extended protection.

Some data breach claims are filed only because notification laws required the company to notify the consumers of the breach, and then the consumers knew to be on the lookout.[44] Companies are not usually operating solely within the borders of one state, and while customers in California may get notified about their breached genetic data,[45] Minnesota residents that have genetic data exposed in the same corporate breach are not required to be notified.[46] This difference in information can lead to varying levels of autonomy in decision making just based on how much information consumers in different states have about data breaches.

Once consumers are aware that certain personal information has been exposed in a breach, then they need to check if fraudulent charges already exist and potentially take mitigating measures to prevent future identity theft.[47] Sometimes companies offer to pay for identity theft protection, sometimes the companies do not.[48] The Federal Trade Commission (FTC) has authority to investigate companies for unfair and deceptive trade practices, which the FTC has used to regulate data privacy and security.[49] Offices of State Attorneys General sometimes pursue companies for data breaches under consumer protection as

43. TEX. BUS. & COM. CODE § 521.002(a)(2) (West 2021).

44. *See, e.g.*, McGeveran, *supra* note 38, at 1148–52 (describing the incentives created for companies by the creation of notification laws); Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 817–21 (describing how notification laws empower citizens to take steps to limit the negative effects of information leakage).

45. CAL. CIV. CODE. § 1798.82(h) (West 2022).

46. MINN. STAT. ANN. § 325E.61(e) (West 2023).

47. Verstraete & Zarsky, *supra* note 44, at 818–20.

48. *See, e.g.*, McGeveran, *supra* note 38 (pointing out the identity protection service costs to some potential disgruntled customers).

49. *Id.* at 1148–53.

well.[50] Consumers can also pursue companies on their own behalf.[51] The private claims are brought under a variety of causes of action: negligence, unjust enrichment, invasion of privacy, and statutory violations.[52]

B. CLASS ACTIONS AFTER DATA BREACHES

After a data breach, if consumers sue a company they are often seeking damages.[53] Among other theories, a frequent damages claim is for the cost of taking mitigating measures to prevent future fraud.[54] The expected damages for mitigating measures for one consumer is a relatively small amount, and an individual consumer lawsuit may not be financially viable.[55] This is why joining a large group of similarly injured people to file suit in a class action makes sense.[56] The increased legal efficiency can help consumers that otherwise would not get redress get their portion of any award that may come out of the case.[57] It also helps companies defend against only one lawsuit, rather than individual suits by each consumer.[58] Many class action lawsuits settle before ever going to trial, but filing a claim does not automatically guarantee a settlement.[59]

In sum, data breaches are an ever-increasing problem for both consumers and businesses. The breaches harm consumers when their PII is exposed and possibly taken advantage of by third parties. The businesses' reputations are tarnished when a breach happens on their watch, and businesses lose money when trying to recover that reputation as consumers come seeking damages. The issue that many consumers face when bringing claims against the breached company is convincing the courts that the consumers have Article III standing.

---

50. *Id.*

51. *See, e.g.*, Megan Dowty, Note, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases,* 90 S. CAL. L. REV. 683, 686 (2017).

52. *Id.*; Mank, *supra* note 7, at 1326.

53. J. Thomas Richie, *Data Breach Class Actions*, BRIEF, Spring 2015, at 12, 14.

54. *Id.*

55. *What Is a Class Action Lawsuit?,* CLASSACTION.ORG, https://www.classaction.org/learn/what-is-a-class-action [https://perma.cc/A7VX-NFF5] .

56. *Id.*

57. *See id.*

58. *See id.*

59. *See How Class Actions Work*, CLASSACTION.ORG, https://www.classaction.org/learn/how-lawsuits-work [https://perma.cc/DM3Z-M6XS].

II. HISTORY OF ARTICLE III STANDING

To bring suit in federal court, the claim must be an actual case or controversy determined through a constitutional doctrine known as Article III standing.[60] Article III standing doctrine is aimed at preventing the judicial process from overtaking the powers of the executive and legislative branches.[61] The doctrine has been built up over time through Supreme Court cases that have created a vague multi-factor test to determine when a plaintiff has standing to bring suit. Article III standing requires that (1) the plaintiff has suffered an injury-in-fact that is: (a) concrete, (b) particularized, and (c) actual or imminent; (2) the injury was likely caused by the defendant; and (3) the injury would likely be redressed by judicial relief.[62] This section will focus on what is required to qualify as an actual or imminent injury-in-fact.

An actual injury-in-fact is relatively straightforward. This requires that the plaintiff suffered an actual harm.[63] Caselaw also allows that if a threatened injury is imminent, defined as certainly impending or a substantial risk of occurring, then it also constitutes an injury-in-fact.[64] An imminent injury-in-fact must be more than an objectively reasonable likelihood to occur, but the Supreme Court has not set an exact bar.[65]

One of the prominent Supreme Court cases regarding imminent injury is *Clapper v. Amnesty International USA*.[66] This case sought injunctive relief against U.S. government wiretaps based on the substantial risk of future harm if the government listened to confidential communications that could potentially be recorded.[67] The fear of harm in *Clapper* was based on five, sequential, hypothetical events occurring and those events causing

60. *See* U.S. CONST. art. III, § 2; Spokeo Inc. v. Robins, 578 U.S. 330, 338 (2016) ("Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy. The doctrine developed in our case law to ensure that federal courts do not exceed their authority as it has been traditionally understood.").

61. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).

62. *Spokeo*, 578 U.S. at 339.

63. *Clapper*, 568 U.S. at 408–10.

64. Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (citing *Clapper*, 568 U.S. 398).

65. *Clapper*, 568 U.S. at 401.

66. *Id.* at 408–10.

67. *Id.*

harm.[68] The court did not find this logic convincing and held that it was not an imminent injury-in-fact because plaintiffs had failed to show that the risk was certainly impending and relied on too much speculation.[69] Thus, the court did not find Article III standing.[70]

Additionally, the court held that a plaintiff cannot "manufacture standing" by choosing to incur mitigation costs against a hypothetical future harm that is not certainly impending.[71] Basically, if a plaintiff buys an umbrella (mitigation) based on a ten percent chance of rain (risk of future harm) the court would likely find that it is a too remote risk of rain for the plaintiff to recover the cost of buying that umbrella. If a court determines that the risk was too low of a likelihood to occur, then mitigation costs for fear of harm will not be considered an actual harm.

More recently, the Supreme Court attempted to clarify what constitutes an injury-in-fact for Article III standing in *TransUnion, LLC v. Ramirez*.[72] When creating consumer reports, TransUnion checked the first and last name of individuals against a U.S. government terrorist watch list.[73] If the first and last name matched the name of a suspected terrorist, TransUnion marked the consumer as a potential terrorist in the company's consumer report.[74] The class members had been incorrectly marked as terrorists in the defendant's database and brought the lawsuit under the Fair Credit Reporting Act (FCRA)

68. *Id.* at 410 ("[R]espondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.").

69. *Id.*

70. *Id.*

71. *Id.* at 402, 416.

72. 141 S. Ct. 2190, 2203 (2021).

73. *Id.*

74. *Id.* at 2201.

for TransUnion failing to keep accurate information.[75] The Supreme Court divided the class into two categories.[76] The Supreme Court found standing for the first 1,853 class members that had their incorrect terrorist data disseminated to third parties, such as a car dealership when applying for a car loan.[77] TransUnion possessed the incorrect data for the remaining 6,332 class members, but the false data had never been seen by a third party.[78] The second group of class members based their standing argument on the substantial risk of future harm of defamation from the existence of incorrect data in the TransUnion internal database.[79]

Writing for the majority, Justice Kavanaugh stated that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm . . . unless the exposure to the risk of future harm itself causes a *separate* concrete harm."[80] The Supreme Court clarified that the difference from *Clapper* is that the earlier case was seeking injunctive relief, and *Ramirez* dealt with damages.[81] Justice Kavanaugh explained that the plaintiffs presented too speculative of evidence to create a substantial risk.[82] This creates a potential new wrinkle in data breach issues because most times when a consumer is suing under a theory of substantial risk of future identity theft, the suit is seeking damages, not injunctive relief. Injunctive relief isn't always the most helpful remedy after a data breach because the company already lost the consumer data, and a court telling the company to stop possessing the consumer data doesn't put the genie back in the bottle.

Spokeo and *Clapper* ushered in a new era of attempted analyses on the nuanced constitutional doctrine of Article III standing.[83] The most recent case, *Ramirez*, did not clear up in what situations an injury may be "imminent" rather than "actual," yet

75. *Id.* at 2200.
76. *Id.* at 2209.
77. *Id.* at 2201, 2209.
78. *Id.*
79. *Id.*
80. *Id.* at 2210–11 (emphasis in original).
81. *Id.* at 2210.
82. *Id.* at 2212.
83. *See, e.g.*, Leading Cases, *Article III Standing—Separation of Powers—Class Actions*—TransUnion v. Ramirez, 135 HARV. L. REV. 333, 336 (2021); David W. Opderbeck, *Current Developments in Data Breach Litigation: Article III Standing after* Clapper, 67 S.C. L. REV. 599, 601 (2016).

still be considered an injury-in-fact for standing. Article III standing analysis now appears to require much more than the first three part test of judicial redressability, causation by defendant, and an injury-in-fact.[84] Injury-in-fact includes its own three part test of particularity, concreteness, and finding an actual or imminent injury.[85] After *Ramirez*, now the analysis requires a further look to find both an imminent injury and a separate concrete harm in order to find standing for damages.[86] Article III standing doctrine is messy, complicated, and frustrating but an instrumental part of federal court cases. Data breach cases are no exception, and Article III standing plays a pivotal role in their development.

III. DEVELOPMENT OF DATA BREACH STANDING IN FEDERAL COURT

In many data breach litigation claims, plaintiffs whose data has been exposed but not yet misused face difficulty satisfying Article III standing requirements. At first look, the reviewing circuits have come to diverging theories around standing for exposed but not yet misused personal information. Four circuits have found standing for plaintiffs based on a theory of substantial risk of future injury.[87] Five circuits have not found standing when presented similar theories.[88] The other three circuits have not yet presided over cases with a question presented on substantial risk of identity theft.[89] Over the years, courts and academics alike have even disagreed over whether these cases should be considered a circuit split.[90]

---

84. Spokeo, Inc. v. Robins, 578 U.S. 330, 339 (2016).

85. *Id.*

86. *Ramirez*, 141 S. Ct. at 2210.

87. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015); *In re* Zappos.com, Inc., 888 F.3d 1020, 1026 (9th Cir. 2018); Attias v. CareFirst, Inc., 865 F.3d 620, 623 (D.C. Cir. 2017).

88. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295 (2d Cir. 2021); Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011); Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017); *In re* SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017); Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332 (11th Cir. 2021).

89. The First, Fifth, and Tenth Circuits.

90. *Compare Beck*, 848 F.3d at 273 ("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."), *and* Antonucci et al., *supra* note 10, at 42 ("Federal courts across the country are not close to reaching a consensus in the

All nine circuits that have reviewed data breach standing cases have had similar enough underlying logic that, after the *Ramirez* decision, Article III Standing in data breach litigation could turn into a cohesive national framework in short order if approached correctly.

A. CIRCUITS FINDING STANDING FOR INDIVIDUALS WITHOUT MISUSE: SIXTH, SEVENTH, NINTH, AND D.C.

The Sixth, Seventh, Ninth, and D.C. Circuits all allowed variations of a substantial risk of future identity theft or fraud to suffice for Article III standing.[91] All four circuits had cases in front of them where a portion of the data breach victims had already suffered actual misuse. The courts explicitly state that evidence of misuse was not a requirement, but they found the presence convincing of the other class members' risk levels. The cases had all different types of data exposed, some mainly dynamic PII and some static PII.[92]

---

hotly contested area of Article III standing in cyber-breach cases."), *with McMorris*, 995 F.3d at 300 ("Some courts have suggested that there is a circuit split on the issue . . . . But in actuality, no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft . . . .") (citations omitted), *and* Devin Urness, Note, *The Standing of Article III Standing for Data Breach Litigants: Proposing a Judicial and a Legislative Solution*, 73 VAND. L. REV. 1517, 1532 (2020) ("The actual 'splits' among the circuits are much smaller than the divergent results suggest.").

91. *See Attias*, 865 F.3d at 623 ("[T]hey provided personal information to the company, including their names, birthdates, email addresses, *social security numbers*, and credit card information.") (emphasis added); *Galaria*, 663 F. App'x at 386 ("The data include names, dates of birth, marital statuses, genders, occupations, employers, *Social Security numbers*, and *driver's license numbers*.") (emphasis added); *Remijas*, 794 F.3d at 690 ("On February 4, 2014, Michael Kingston, the Senior Vice President and Chief Information Officer for the Neiman Marcus Group, testified before the United States Senate Judiciary Committee. He represented that 'the customer information that was potentially exposed to the malware was payment card account information' and that 'there is no indication that social security numbers or other personal information were exposed in any way.'"); *In re* Zappos.com, Inc., 888 F.3d at 1029 ("Plaintiffs have sufficiently alleged an injury in fact based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft.") (footnote omitted).

92. *See supra* Part I.A.1. Dynamic PII is information that could be feasibly changed by a consumer like a credit card number or account password. Static PII is information that cannot be so easily changed like a social security number, full name, or biometric data.

Plaintiffs filed the Sixth Circuit case *Galaria v. Nationwide Mutual Insurance Co.* after hackers breached the company's network and stole mostly static PII belonging to the consumers.[93] The named plaintiff, Galaria, alleged actual misuse of data in three unauthorized attempts to open credit cards in his name.[94] The court found that the plaintiffs had Article III standing by looking to the substantial risk of harm coming from the exposure of static PII combined with "reasonably incurred mitigation costs."[95] The court went out of its way to prove the risk went beyond mere speculation 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."[96]

In the Seventh Circuit *Remijas* case, hackers breached the defendant's network and exposed the plaintiffs' dynamic PII.[97] There was no indication the breach exposed any static PII other than names.[98] A sizable number of the plaintiffs alleged that they had already suffered fraudulent charges but were additionally suing to recover for future harms and mitigation costs.[99] The court held that the risk was not too speculative and was plausible to infer that a substantial risk of harm existed after the breach.[100] The plausible inference was sufficient to survive a motion to dismiss for lack of standing.[101]

The plaintiffs in the Ninth Circuit filed suit after hackers gained access to the information of 24 million customers of Zappos.com.[102] The breach included names and addresses, but otherwise dynamic PII, like credit card information, passwords, and email addresses.[103] Only plaintiffs that had not alleged actual

93. This included full names, DOB, SSN, driver's license number, gender, employer, occupation, and marital status. *Galaria*, 663 F. App'x at 386.

94. *Id.* at n.1.

95. *Id.* at 388.

96. *Id.*

97. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015) (acknowledging that payment card account information was exposed).

98. *Id.* (noting specifically that SSN was not part of the breach).

99. *Id.* at 692.

100. *Id.* at 693 ("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.").

101. *Id.*

102. *In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018).

103. *Id.* at 1023.

misuse were on appeal, but a portion of the class received standing at the district court who alleged actual misuse.[104] The court held that the plaintiffs in *Zappos* had standing based on the substantial risk that the hacker would commit identity fraud or theft with the information compromised.[105] The court acknowledged that no SSNs were compromised and highlighted that the passwords were a cause for risk.[106]

The D.C. Circuit case presented plaintiffs that had both dynamic and static PII exposed through a hack.[107] The court cited to *Remijas* and agreed that this case did not include a "long sequence of uncertain contingencies" and was at least plausible as a substantial risk and sufficient for an injury-in-fact.[108]

While these circuits all held there is standing based on the theory of substantial risk of future identity theft, the main similarity was evidence of misuse, and there was a lack of emphasis on the type of data compromised. In reviewing circuit decisions that have denied standing, it will become evident that the decisions of the cases vary because of the facts and not because of an insurmountably large gap in underlying logic in the circuits.

B. CIRCUITS THAT DID NOT FIND STANDING WHEN LACKING MISUSE: SECOND, THIRD, FOURTH, EIGHTH, AND ELEVENTH

The Second, Third, Fourth, Eighth and Eleventh Circuits have also reviewed cases presenting a theory around substantial risk of future identity theft from compromised data.[109] These circuits denied standing for the class members that did not allege actual misuse, but some of the circuits agreed with the general theory of increased risk being sufficient.[110] The courts held that

104. *Id.* at 1027.

105. *Id.*

106. *Id.*

107. The static PII included names, DOB, and SSN. Attias v. CareFirst, Inc., 865 F.3d 620, 623 (D.C. Cir. 2017). The dynamic PII included credit card information. *Id.*

108. *Id.* at 628–29.

109. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 298 (2d Cir. 2021); Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1335 (11th Cir. 2021); *In re* SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017); Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017); Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011).

110. *See, e.g.*, *McMorris*, 995 F.3d at 300–01 ("We therefore join all of our sister circuits that have specifically addressed the issue in holding that plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data.").

on the facts in front of them there was no standing.[111] The main difference for some of these cases from those finding standing was a focus on the lack of intentionality, meaning courts felt they needed to see evidence of hackers/bad actors (non-parties to the suit) intending to misuse the data for it to create a risk.

In 2011, the Third Circuit decided one of the earlier data breach cases in *Reilly*.[112] The defendant company suffered a security breach and the hacker gained access to both static and dynamic PII.[113] The court explicitly pointed out that it was not known whether the hacker read, copied, or understood the data.[114] No plaintiffs alleged any actual misuse.[115] The court held that there was no standing based on risk of future injury because the theory was too attenuated being dependent on "speculative, future actions of an unknown third-party."[116] The court found important the lack of proof that the hacker took or understood the data compromised during the breach, and stated there was only proof that something penetrated a firewall.[117]

The Fourth Circuit reviewed a case in 2017 over the physical theft of a laptop with unsecured data.[118] The data on the laptop included static and dynamic PII, including medical information of over 7,000 patients.[119] Plaintiffs did not allege actual misuse.[120] The Fourth Circuit held that a threatened event could be a "reasonable risk" to occur but still be insufficient to constitute a substantial risk of harm.[121] In other words, while the data on the laptop posed a reasonable risk of harm to the plaintiffs, the court held there was not standing because there was no allegation of actual misuse of the data nor evidence presented that the thief intended to misuse the PII.[122] Accordingly, the court held

111. *Id.*

112. 664 F.3d at 38.

113. *Id.* at 40 (including names, SSN, and for some people date of birth (DOB) and direct deposit bank account).

114. *Id.*

115. *Id.*

116. *Id.* at 42.

117. *Id.* at 42–44.

118. Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017).

119. *Id.* at 267 (including name, DOB, last four digits of SSN, height, weight, and gender).

120. *Id.*

121. *Id.* at 276.

122. *Id*. at 274 (describing how sister circuits that found there was an imminent risk did so for cases that alleged misuse or could point to the intent of the theft).

that there was a reasonable risk that theft of the laptop could result in identity theft but did not find Article III standing.[123]

In the Eighth Circuit, the court reviewed a case where the plaintiffs' information was breached in a hack on defendant's database.[124] The information included dynamic PII and full names.[125] One plaintiff alleged an actual injury of fraudulent charges, and the court granted only that plaintiff Article III standing.[126] The Eighth Circuit held that compromised credit card information without any other personal information was insufficient to create a substantial risk of harm constituting an injury in fact.[127]

The Eleventh Circuit is one of the most recent circuits to join the fray in data breach standing with the *Tsao* case, decided in February 2021.[128] In *Tsao*, a hacker gained access to the defendant's database and obtained dynamic PII in credit and debit card information.[129] The plaintiff received notice from the defendant of the breach and immediately cancelled both impacted cards.[130] The court cited the 2007 GAO Report[131] pointing out that without additional static PII the only risk from credit card information is for that card to be charged.[132] By cancelling the cards, the plaintiff had ensured there was no future risk of identity theft and the court held there was not standing.[133]

Another of the most recent circuit decisions on data breach standing came from the Second Circuit in April of 2021 in *McMorris v. Carlos Lopez & Associates, LLC*.[134] The plaintiffs were all current or former employees of the defendant.[135] The

123. *Id.* at 276.

124. *In re* SuperValu, Inc., 870 F.3d 763, 765 (8th Cir. 2017).

125. *Id.* at 766 (including credit/debit card account numbers, expiration dates, CVV codes, and PINs).

126. *Id.* at 772.

127. *Id.* at 771–72.

128. Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332 (11th Cir. 2021).

129. *Id.* at 1335 (including expiration dates, CVV, and PINs).

130. *Id.*

131. *See* GAO REPORT 2007, *supra* note 30.

132. *Tsao*, 986 F.3d at 1342 ("That [GAO] report points out, however, that compromised credit or debit card information, without additional personal identifying information, 'generally cannot be used alone to open unauthorized new accounts.'").

133. *Id.* at 1342–45.

134. 995 F.3d 295 (2d Cir. 2021).

135. *Id.* at 298.

company sent an accidental email out to current employees that exposed both static and dynamic PII of the class members.[136] No class members alleged that anyone outside the company obtained the data.[137] There were no allegations that any plaintiff had suffered actual harm from the data exposure.[138] The Second Circuit in *McMorris* did not find standing for the class members in front of the court, but held that there could be standing based on an increased risk of future identity theft or fraud in other circumstances.[139] The court mentioned that maybe the outcome would have been different if there had been allegations of malicious intent by those that obtained the PII or if there were allegations of actual misuse by some of the class members.[140] The *McMorris* decision came out prior to *Ramirez*, and remains good law until the Second Circuit decides otherwise.[141] The only other circuit that has addressed something close to standing based on an imminent injury after a data breach is the First Circuit in *Katz v. Pershing, LLC*.[142] The plaintiff brought the claim against a company that kept poor security maintenance of its e-platform, but no breach had occurred.[143] The court held that there was not a substantial risk of injury sufficient to find Article III standing, but this was not regarding an actual breach, only a data exposure.[144]

In sum, four circuit courts found standing for class members that did not have actual misuse, and in every case a fellow class member alleged actual misuse, but only two cases included static PII.[145] Five circuits did not find standing for class members with exposed data and no misuse; only four of those cases involved actual breaches and of those four only one included static PII.[146] U.S. circuits possess varied precedent from various factual bases

136. *Id.*

137. *Id.*

138. *Id.*

139. *Id.* at 300–01.

140. *Id.* at 302–05.

141. Cooper v. Bonobos, Inc., No. 21-CV-854, 2022 WL 170622, at *3 n.1 (S.D.N.Y., Jan. 19, 2022) ("[I]t is the task of the Second Circuit, not this Court, to determine if *McMorris* should be overturned."); *McMorris*, 995 F.3d 295 (2d Cir. 2021); TransUnion, LLC v. Ramirez, 141 S. Ct 2190 (2021).

142. 672 F.3d 64 (1st Cir. 2012).

143. *Id.* at 80.

144. *Id.*; *see supra* Part I.A.1.

145. *See supra* Part III.A.

146. *See supra* Part III.B.

when dealing with data breach victim Article III standing. Circuits have focused their standing analyses on the type of data compromised, the intentionality of the third party, and the presence of class members with actual misuse. While almost all the courts have similar underlying logic, there have been diverse weights given to each of the three factors. In light of *Ramirez*, plaintiffs' success in establishing standing based on risk of identity theft might appear bleak.

IV. FINDING COMMON GROUND AMONG THE CIRCUITS AND WHAT *RAMIREZ* MEANS FOR DATA BREACH STANDING

Ramirez held that an imminent injury-in-fact is not sufficient for standing in a case for damages unless there's a connected concrete harm,[147] but this hasn't yet been widely applied at the appellate level to data breach cases. The various circuit decisions discussed above could be viewed as almost in alignment, but it's possible the differences are exacerbated without proper foresight in applying *Ramirez*.

A. *MCMORRIS* GIVES GENERAL OVERVIEW OF THOUGHT PROCESSES BEFORE *RAMIREZ*

In *McMorris*, the Second Circuit put together a robust summary of the common themes among its sibling circuits in determining standing in data breach cases.[148] The court highlighted three main themes throughout court analysis: the intent behind the data breach, evidence of misuse, and the type of data at issue.[149]

First, the court cites intent as a factor, but really what the court appears to be going after is distinguishing between a data exposure (an accidental company email) and a data breach (hack).[150] The court wonders why else would any hacker, a "malicious third party," break into a database except for future identity theft, implying that any cyberattack before the court would not have any issues proving intent.[151] The only case involving a

147. *See supra* Part II; TransUnion, LLC v. Ramirez, 141 S. Ct. 2190, 2203 (2021).

148. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301 (2d Cir. 2021).

149. *Id.* at 300–01.

150. *See supra* Part I.A.

151. *McMorris*, 995 F.3d at 301.

hacker where intent played a significant role in the outcome was *Reilly*.[152] The court focused on the unknown of whether the hacker read, copied, or understood the data.[153] Since that opinion in 2011, circuit court decisions have not focused on questioning the ability of hackers to understand how to take advantage of consumer personal information. This is likely because in the last decade it has become clear that if the hackers cannot use data themselves, there is an illicit market to sell that information to someone who can use it.[154]

Second, the court in *McMorris* claims that evidence of misuse is not a necessary component of standing.[155] Both the court in *McMorris* and the author of this Note cannot cite any case that found standing based on substantial risk without some class members presenting evidence of misuse. Some observers might view this as a contradiction. Courts are stating that actual misuse is not necessary for standing, but then strongly emphasize evidence of misuse in decisions and never find standing without actual misuse.[156] This shows the uncertainty and gray area left in data breach caselaw. The only way courts are finding a clear and substantial risk of harm is when presented with actual identity theft or fraud. This seems in need of clarification.

Third, the focus on the type of data is an important aspect of this analysis. PII has a fluid definition that almost every state and data scholar views slightly differently.[157] Almost all agree that static PII, information that is hard for individuals to change and allows thieves to open new accounts, is dangerous when in

152. Reilly v. Ceridian Corp., 664 F.3d 38, 42–44 (3d Cir. 2011).

153. *Id.*

154. *See supra* Part I.A; *see, e.g.*, Edvardas Mikalauskas, *What's Your Identity Worth on the Dark Web?*, CYBERNEWS (Sept. 28, 2021), https://cybernews.com/security/whats-your-identity-worth-on-dark-web [https://perma.cc/SD5B-HZMT].

155. *McMorris*, 995 F.3d at 301 ("[W]hile not a necessary component of establishing standing, courts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused.").

156. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386, 388 (6th Cir. 2016) (stating that it would be unreasonable requiring plaintiffs to wait for actual misuse to bring suit, but the named plaintiff alleged actual misuse); *McMorris*, 995 F.3d at 301–02 ("[A]llegations that other customers whose data was compromised in the same data breach had reported fraudulent charges on their credit cards helped establish that the plaintiffs were at a substantial risk of future fraud.").

157. *See supra* Parts I.A.1 & I.A.2.

the wrong hands, but there's disagreement on how much risk static PII alone creates.[158]

The confusing portion of this difference in judicial logic is that in some jurisdictions the risk of future identity theft is substantial enough that mitigation efforts may be recovered as damages.[159] Whereas in other jurisdictions, the courts have decided that risk of identity theft is not substantial enough for standing, meaning that mitigation efforts are not compensable as damages.[160] Plaintiffs who have undergone mitigation efforts are accused of using such efforts to manufacture standing.[161] This means that undergoing mitigation efforts after a data breach for one portion of U.S. citizens could result in getting it paid back by the company that lost the data. The other portion of the country will never be reimbursed. The location of the data breach class action significantly impacting the outcomes is likely to lead to frustrated citizenry and could incentivize forum shopping.[162]

It appears the Supreme Court does not yet feel the need to address the standing issue in data breach litigation.[163] Now that there has been an update on Article III standing analysis through *Ramirez*, it is possible that: (1) the circuits all find common ground on their own, (2) the Supreme Court will finally grant review on data breach standing, or (3) everyone continues muddling through the murky uncertainty of Article III standing doctrine. Most likely for the near future is the latter, as those involved in data breach cases are left to fend for themselves and each district court will rely on disparate caselaw to find some sort of resolution.

158. *See supra* Part III.A.

159. *See supra* Part III.A.

160. *See supra* Part III.B.

161. *See supra* Part III.B.

162. "Forum Shopping" refers to the strategy of picking which district to file based on the advantages of the caselaw.

163. *In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019); Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017), *cert. denied*, Beck v. Shulkin, 137 S. Ct. 2307 (2017); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011), *cert. denied*, 566 U.S. 989 (2012).

B. *RAMIREZ* PROVIDES INTERESTING CROSSROADS IN DATA BREACH STANDING; WILL THE IMMINENT INJURY-IN-FACT THEORY BE RETIRED?

While the Tenth Circuit has not yet made a decision related to data breach standing, a recent case out of the Western District of Oklahoma—part of the Tenth Circuit—bears mentioning. The court decided *Legg v. Leaders Life Insurance Co.*, which serves as the first data breach litmus test after the June 2021 Supreme Court decision of *TransUnion, LLC v. Ramirez*.[164] The *Legg* case involved a third party intentionally breaching and removing files with static PII.[165] The court in *Legg* determined that, based off the reasoning of *Ramirez*, the data lost in a breach could not confer standing using a substantial risk of future of identity theft.[166] The Western District of Oklahoma reasoned that "risk of future harm alone cannot support standing for a damages claim" and claimed there were too many layers of speculation to be certainly impending.[167] The plaintiffs had alleged mitigation costs, but the court only found that mitigation costs were not able to manufacture standing.[168]

The *Ramirez* decision is not as dispositive as the Western District of Oklahoma made it out to be in *Legg*.[169] The plaintiffs who were denied standing in *Ramirez* never had their data exposed to a third party, and the risk of future harm alleged was that it may someday be given to a third party.[170] The facts in *Ramirez* line up more with the *Katz v. Pershing* case, where there had not yet been an actual data breach, just poor security.[171] These are both attenuated situations where no third party has gained the data. But where there's been a data breach the third party already has the data.

Further, the clarification given on Article III standing by the Supreme Court in *Ramirez* does not mean that data breach claims are dead in the water until there has been actual misuse.

---

164. Legg v. Leaders Life Ins. Co., 574 F. Supp. 3d 985 (W.D. Okla. 2021); TransUnion, LLC v. Ramirez, 141 S. Ct. 2190 (2021).

165. *Legg*, 574 F. Supp. 3d at 987–88 (including names, DOB, SSN, and Tax ID).

166. *Id.* at 992–94.

167. *Id.* at 993, 995.

168. *Id.* at 994.

169. *Ramirez*, 141 S. Ct at 2190; *Legg*, 574 F. Supp. 3d at 985.

170. *Ramirez*, 141 S. Ct. at 2211.

171. Katz v. Pershing, LLC, 672 F.3d 64, 78 (1st Cir. 2012); *see supra* Part III.B.

In *Ramirez*, the Court said that risk of future harm was not sufficient unless the risk caused an injury in and of itself.[172] Data breach cases are different than *Ramirez* because the information in a data breach has already been exposed to a third party and taking mitigating measures to prevent identity theft costs actual money, thus constituting an injury. However, a flaw is that mitigating measures do not create standing for a risk that is not already certainly impending.[173] So long as no one knows exactly where the line is for certainly impending risk of identity theft, then there is a danger that the consumers who have been harmed in a way that federal courts can address are not able to file suit.

Imagine Consumer 1 gives their home address, SSN, date of birth, and credit card information to Company A, and Consumer 2 gives the same data to Company B. The data at both companies is compromised, and the consumer PII is exposed in the hack. Consumer 1 hears of the breach and fearing identity theft pays for protection. Consumer 2 also hears of the breach and fears identity theft but cannot or does not want to front the cost of protection and wants the company to pay for it. Both consumers then sue the companies as part of class actions. Under the current confusing regime, both consumers may believe that they have standing to bring the case in federal court. However, under *Ramirez* it's entirely possible that Consumer 1 receives no standing because it is decided that the risk was not certainly impending, and thus the mitigating costs were not an actual injury, but merely an attempt to manufacture standing. Consumer 2 also receives nothing, because although the static PII may create a substantial risk of future injury, there is not another injury alleged. If Consumer 2 had known that they needed to have already paid protection costs in order to recover in court, they would have been more likely to have paid for protection out of pocket.

If there were a clear delineation for "certainly impending" in data breach cases, consumers would know exactly when there was standing under a substantial risk of identity theft. That clear knowledge would allow for mitigation measures to be taken appropriately, creating a concrete injury out of the risk. The line should be drawn to allow for a data breach victim, with no evidence of misuse, to have standing on the theory of future risk of

172. *Ramirez*, 141 S. Ct. at 2210–12.

173. *See supra* Part II.

identity theft or fraud. This is still in line with the decision in *Ramirez* and should be solidified into an understandable rule across federal jurisdictions.

V. COURTS SHOULD ADOPT A DATA TYPE-BASED RULE IN ANALYZING DATA BREACH STANDING ANALYSIS

Most of the proposed solutions have focused on balancing a series of factors to get to the bottom of data breach standing.[174] And while these multi-factor tests allow for detailed analysis of each individual case, the lack of clear rules creates uncertainty for data breach victims regarding when they actually have standing to go to court. Article III standing is already a multi-part test, and data breach litigation does not need to add its own multi-factor test inside the injury-in-fact prong of standing. Consumers need an easy-to-understand rule for Article III standing in data breach cases so that mitigation measures can be taken when appropriate and still satisfy the requirements of *Ramirez*. This Note proposes a bright line rule focused on the type of data in the breach as sufficient to confer standing allowing for greater clarity to consumers, businesses, and courts going forward.

A. RULES VS. STANDARDS, FOR DATA BREACHES A RULE WOULD WORK BETTER

Within the broader context of legal theory, there is a balancing act by legislatures and courts alike between focusing on the use of rules or standards.[175] Rules provide more certainty and restraint of official arbitrariness through clear cut application.[176] Whereas standards allow for more nuance to be placed into the decision process.[177] Another distinguishing factor is the cost of administrability.[178] Rules are easier to administer, but may get the outcome wrong more frequently.[179] Standards are

174. *See, e.g.*, Dowty, *supra* note 51, at 701 (proposing standing for "reasonable and substantial sorting-things-out costs" but not for all risk of future identity theft); Urness, *supra* note 90, at 1553 (proposing a three-factor test for intent, evidence of misuse, and nature of disclosed information).

175. Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685, 1687, 1696 (1976).

176. *Id.* at 1688.

177. *Id.* at 1689–99.

178. *See id.* at 1685 (noting the high degree of administrability for formal rules).

179. *Cf. id.* (noting the tension between the law's efforts to apply rigid, uniform rules and the desire to reach equitable, socially beneficial outcomes).

hopefully more accurate than rules, but are more difficult to administer.[180] An example of a rule would be *Miranda* rights, where police must inform a suspect of their rights prior to interrogation.[181] An example of a standard would be good faith, where parties to a contract are expected to have negotiated in good faith and can be found in breach of contract by a judge for violating the standard.[182]

Both rules and standards have their place in legal decision making depending on the time, place, and goals of the situation. While standards allow for more judicial discretion and flexibility, they can lead to more confusion for the average citizen without an in-depth legal education.[183] Rules tend to lead to more certainty in public understanding.[184] This Note proposes that data breach litigation needs one clear rule for imminent injury-in-fact inside the larger Article III standing analysis, providing consumers with a clearer understanding and courts with a quicker decision process.

B. THE PROPOSED DATA TYPE RULE

This Note proposes that rather than looking at all these various standards and non-exhaustive factors, there should be a clear-cut rule. This would allow for courts to be consistent, and for plaintiffs to understand more about data breach litigation. This is not to argue that these are simple situations that do not require thought, but that standing should not—and need not—create so much hang-up in data breach litigation.

The only fact of significance for standing in data breach litigation should be what type of data has been exposed in the breach. If static PII is exposed in a breach, then that should be enough to create a substantial risk of future identity theft that meets the imminent injury-in-fact requirement of Article III standing.[185] This is not an attenuated chain of possibilities; the

180. *Cf. id.* at 1699–70 (outlining the assumptions behind preferring rules over general or flexible standards).

181. *Id.* at 1706 n.59 (using the Miranda Rights as an example of a rule); Miranda v. Arizona, 384 U.S. 436, 455–70 (1966) (laying out a set of immutable requirements).

182. Kennedy, *supra* note 175, at 1688.

183. *See id.* at 1710 (summarizing the pros and cons of rules and standards).

184. *See id.* at 1688 ("[I]f private actors can know in advance the incidence of official intervention, they will adjust their activities in advance to take account of them.").

185. *See supra* Parts I, II & III.

static PII is out there and available for use or sale by nefarious parties.[186] This static PII is sensitive information that is not easily changed and would include items such as a Social Security Number and biometric data.[187] When connected with a name, these would be considered "high-risk information" similar to the Second Circuit's holding in *McMorris*.[188] High-risk information allows would-be thieves to open new accounts in a person's name, which is a greater risk than being able to use already existing accounts when thieves gain access to only dynamic PII.[189]

This proposed data type rule favors predictability over a larger sense of particularized fairness to companies. While some companies may have followed every best practice known to security professionals, there could still have been a data breach.[190] This leads some academics and companies alike to argue that, in fairness, those companies should not be punished for their "bad luck" of getting hacked.[191] However, focusing on predictability and certainty allows companies to know that if they are storing certain data on customers and the company is breached, those individuals will have standing. However, this is not to say that the consumers automatically have a suit that requires payout. Standing is the first procedural hurdle in a legal claim that moves to higher and higher burdens of proof before finding liability. Admittedly, many class actions settle before ever getting to trial, but the judge must issue an order approving the settlement.[192]

This predictability would incentivize companies to store less sensitive information about their clients to avoid lawsuits stemming from "inevitable" data breaches.[193] This will force innovation, as companies try to get the same profit outcomes and create new market spaces while trying to reduce the sensitivity of consumer data they store. Given that many professionals view data breaches as inevitable, the solution is not to provide companies a middle ground where they (1) host personal information, (2) lose it in a breach (that they knew was coming), and (3) are

186. *See* Mikalauskas, *supra* note 154.

187. *See supra* Part I.A.

188. *See* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 302 (2d Cir. 2021); *see also supra* Part IV.A.

189. *See supra* Part I.

190. *See* Verstraete & Zarsky, *supra* note 44, at 839.

191. *Id.*

192. *See supra* note 59 and accompanying text.

193. Verstraete & Zarsky, *supra* note 44, at 840.

not held liable in court because the company took reasonable security precautions. When the static PII is out there, people are now at risk of harm because the company chose to retain that information.

Additionally, creating a brighter line on Article III Standing for data breaches would likely incentivize companies to improve their security practices. If the company chooses not to end the collection of static PII and there is no longer a protection from liability based on following industry security standards, then there's a strong chance companies would be encouraged to go above and beyond standard security to protect the consumer data.

This argument may seem callous to the needs of businesses, through risking higher litigation costs and higher costs of database maintenance. However, it seems only fair that companies that are profiting off the use of consumer personal information[194] should need to treat the long-term storage of that data as a last resort rather than a default.

C. OTHER FACTORS ARE NOT NECESSARY TO DETERMINE STANDING

The other non-exhaustive factors besides data type that courts and scholars have recommended include intent and evidence of misuse.[195] Courts have referenced the factors in varying depth and found the factors convincing in other cases.[196] Both of these inquiries could be useful to a plaintiff in providing more context in a complaint, but neither should be necessary inquiries for a court to find an injury-in-fact for standing.

Intent of hackers is not worth pursuing for a judge at the standing inquiry because the hackers are not parties to the suit,

194. *See, e.g.*, Max Freedman, *How Businesses Are Collecting Data (and What They're Doing with It)*, BUS. NEWS DAILY (Jan. 23, 2023), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/43MR-E37N] (talking about how a primary reason businesses collect data is to transform it into a cashflow).

195. *See* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 303 (2d Cir. 2021) (laying out three non-exhaustive factors for courts to evaluate a plaintiff's standing); Urness, *supra* note 90, at 1520 (discussing intentionality of breach, nature of information disclosed, and evidence of misuse as factors courts have considered).

196. *See supra* Part III.

and the analysis quickly gets too abstract.[197] Judges are not required to be proficient in computer science or the Dark Web.[198] By requiring a judge to look to the steps of intent for a hacker, this type of standard may risk causing an inefficient factual investigation. In *Reilly,* the Third Circuit found that "all that is known is that a firewall was penetrated," and thus held there was no proof of intentional or malicious intrusion.[199] The court used that reasoning in its decision to not confer standing.[200] This 2011 case weighing the impacts of breaching firewalls seems to be the wrong inquiry at the preliminary stage of standing and should be reserved for later in the judicial process. It is better to leave intent of a non-party out of the standing analysis to prevent confusion and overburdening at the pleading stage.

Evidence of misuse can be probative of showing whether the risk of identity theft is real. However, actual misuse should not be necessary to confer standing because the identity theft risk should already be sufficiently shown through the type of data lost. Requiring a part of the class to have already suffered an identity theft goes against the idea of allowing standing when there's an imminent injury. Misuse is an actualized injury-in-fact, and by the Supreme Court's own definition, cases and controversies can be an injury that is actual or imminent.[201]

In sum, evidence of misuse and intentionality should not be required factors when reviewing Article III standing in data breaches. While evidence of misuse is helpful, it could lead to perverse incentives. If a 100% chance of rain is not substantial enough risk to warrant getting reimbursed for an umbrella, then how many people may decide to wait until after the rain starts to buy the umbrella? That goes against allowing people to at-

197. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, TEX. L. REV. 737, 778 (2018) ("Courts should not require proof that hackers had criminal motives. As a practical matter, the hackers' identities are unknown and thus such proof is elusive.").

198. *See, e.g.*, Mikalauskas, *supra* note 154 (describing the "Dark Web" as a key place for solen identity sales).

199. Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011).

200. *Id.*

201. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 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 the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.").

tempt to avoid harm and still have Article III standing. Intentionality can quickly go too abstract and stray away from what should be a preliminary Article III Standing analysis.

D. POTENTIAL COUNTERARGUMENTS DON'T HOLD WEIGHT

Proponents of data protection may disagree with the proposal that credit card information should be left out of the proposed category for high-risk information because fraudulent credit card charges are a harm to consumers. However, this Note is specifically targeting the rule for finding standing under the theory of substantial risk of future identity theft. This is not to say that credit card fraud cannot constitute an actual injury-in-fact itself when it has occurred, but a plaintiff could more easily change their credit card number than file a lawsuit if that's the only data exposed. Not to mention that 15 U.S.C. § 1643 sets a maximum of fifty dollars for consumer liability for unauthorized credit charges.[202]

Organizations can still defeat the claim on causation grounds, if they are able to show that there were other data breaches that included that same alleged information.[203] For example, organizations may argue that different hackers might have stolen plaintiffs' PII in breaches from different companies, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from defendant). However, this argument is less about injury-in-fact standing and more about the merits of causation and damages. The Seventh Circuit recognized in *Remijas v. Neiman Marcus Group, LLC*, that "some other store might [also] have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue" for the breach in question.[204]

In summary, Article III standing is already confusing enough to courts and parties. Data breach litigation does not need its own intricate standard for finding an imminent injury-in-fact. Attempting to justify an intricate standard with a hope of greater accuracy while creating a high cost of administrability

---

202. 15 U.S.C. § 1643 (a)(1)(B).

203. Verstraete & Zarsky, *supra* note 44, at 845 ("Of course, this requires that harms from data breach be traceable to specific breach incidents, which is difficult. Indeed, consumers might attribute identity theft incorrectly or to firms which exposed their information most recently.").

204. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015).

is not convincing. The proposed data type rule focused on static PII for standing analysis would provide a succinct way forward and would not result in a dearth nor surplus of plaintiffs with standing.

VI. HOW TO APPLY AND MOVE FORWARD

With an understanding of this Note's proposed rule for standing in data breach litigation, the final piece to the puzzle is to see what this type of focus on data type would have done in the aforementioned cases.[205] This Part applies the proposed rule to previously discussed circuit cases and provides a call to the GAO to renew their research into data breaches and identity theft.

A. APPLYING THE PROPOSED DATA TYPE RULE

This proposed rule may seem to endanger causing a drastic increase in the number of data breach cases that have standing by opting for a rule over a standard.[206] Looking at the circuit cases retrospectively, this may not prove true prospectively. Applying this data type rule for class members without misuse would have changed the standing analysis outcome for only three of the nine cases discussed above.[207] This new rule would have resulted in three circuits finding standing[208] and six circuits not finding standing.[209] The rule only slightly alters the original decision make-up of four finding standing and five not.[210]

---

205. *See supra* Part V.A.

206. *Cf. supra* Part I.B (noting that data breaches are an "ever-increasing problem"); Part V.B (proposing a bright-line rule based on type of data breached).

207. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); *Remijas*, 794 F.3d 688; *In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018).

208. The Third, Sixth, and D.C. Circuits would have found standing under the proposed rule. *See, e.g.*, *Reilly*, 664 F.3d 38; Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017).

209. The Second, Fourth, Seventh, Eighth, Ninth, and Eleventh Circuits would not have found standing. *See, e.g.*, McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295 (2d Cir. 2021); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017); *Remijas*, 794 F.3d at 688; *In re* SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017); *In re* Zappos.com, 888 F.3d 1020 (9th Cir. 2018); Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332 (11th Cir. 2021).

210. *See supra* Parts II & III.

The Third Circuit in *Reilly* should have found standing because the data breach included names, dates of birth, social security numbers, and bank accounts.[211] This data is static PII that is difficult for individuals to change and easy for thieves to exploit. This meets this Note's proposed threshold for static PII standing.

The D.C. Circuit in *Attias* would still have found standing under this rule because the data in question included names and social security numbers.[212]

The Sixth Circuit in *Galaria* would still have found standing because among other things the data breach included names, Social Security numbers and driver's license numbers.[213]

The Seventh Circuit in *Remijas* should not have found standing because only credit card information was breached.[214] For this proposed rule, credit card information alone is not sufficient. The plaintiffs that did not suffer actual credit card fraud should not have had standing.

The Ninth Circuit in *Zappos* should NOT have found standing for some of the plaintiffs. The data breach included names but mainly dynamic PII, like credit card account information.[215] For the plaintiffs that suffered actual fraudulent charges there would be' standing to bring suit, but under the theory of substantial risk of future harm this Note's proposed rule would preclude any other class members.

The Second Circuit in *McMorris* should still not have found standing because this did not involve a data breach, but merely a data exposure internal to the company and should be subject to more particularity when it comes to standing analysis.[216]

The Fourth Circuit in *Beck* would still not have found standing because of the physical theft of a laptop.[217] This case is not in the same category as a hack, similar to the case above in

---

211. *Reilly*, 664 F.3d at 40 ("[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.") (internal quotations omitted).

212. *Attias*, 865 F.3d at 623.

213. *Galaria*, 663 F. App'x at 386.

214. *Remijas,* 794 F.3d at, 690 (noting specifically that SSN was not part of the breach).

215. *In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018).

216. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 298 (2d Cir. 2021).

217. Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017).

McMorris.[218] Although the information on the laptop included the last 4 digits of SSN and physical descriptors and could be considered static PII,[219] it does not meet this Note's proposed rule of standing for static PII in a data breach because the physical theft does not meet the same level of threat as a hack.

The Eighth Circuit in *Supervalu* was correct in not finding standing because the only information breached was credit card information, which is not considered static PII, and it is easy to thwart a would-be identity thief by changing the card number.[220]

The Eleventh Circuit in *Tsao* should still not have found standing. There was only credit card information—dynamic PII—breached.[221] Without any other data this fails the proposed rule and there's not standing.

While this proposed rule may at first seem to be cause for an increase in caseload, if the outcomes of the analyzed circuit cases are any indication, that may not be the case going forward. If this rule could incentivize more companies to halt storage of static PII that would be better for consumers. The less organizations that have a copy of static PII, the lower likelihood that an individual's PII will be compromised when data is out of the individual's control.

B. THE GAO SHOULD RENEW RESEARCH INTO DATA BREACHES AND IDENTITY THEFTS, PROVIDING A MORE RECENT ANALYSIS THAN 2007

Referenced throughout these data breach decisions, both by plaintiffs and by judicial decisions, is the GAO Report published in 2007.[222] Between 2007 and 2022, there has not been another report published by the GAO on identity theft, while the approximate number of data compromises taking place annually has gone from 570 in 2005–06, to 1,280 in 2018, to 1,862 in 2021.[223]

---

218. 995 F.3d 295 (2d Cir. 2021).

219. *Beck*, 848 F.3d at 267 ("The [stolen] 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).").

220. *In re* SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017).

221. Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1335 (11th Cir. 2021).

222. GAO REPORT 2007, *supra* note 30; *see supra* note 29 and accompanying text.

223. GAO REPORT 2007, *supra* note 30; ITRC REPORT 2020, *supra* note 18; ITRC Report 2021, *supra* note 6.

Courts and plaintiffs alike reference a GAO report on identity theft that reviewed incidents from a different era.[224] Hackers are now able to cause entire pipelines to be shut down[225] and can hack into people's front door cameras.[226] This Note is not arguing that the GAO report is wrong but is questioning how much it can still be trusted given the advancements in technology since the reviewed breaches in 2000 to 2005.

The GAO Report references companies that talk about stolen "data tapes" and suggests that this practice helps prevent misuse because of specialized equipment.[227] Data tapes are no longer a large presence in 2023 companies, and when a business loses the data of 24 million consumers, it is not on physical tapes.[228]

A renewed effort by the federal government to reassess the impact of data breaches and identity theft on consumers would be helpful to the courts and citizenry. With technology advancing so quickly, courts should not be referencing studies about data breaches that stopped looking at data before Twitter was founded.[229] In fact, courts are on board with new studies,[230] unfortunately it's not for the courts to start the process. The rest of the government should refocus efforts at looking at the impact of

---

224. *E.g.*, *Tsao*, 986 F.3d at 1343 ("Of course, we recognize that the GAO Report is over a decade old, and it is possible that some breaches may present a greater risk of identity theft than others.").

225. *E.g.*, William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [https://perma.cc/KYV9-JFGS].

226. Kari Paul, *Dozens Sue Amazon's Ring After Camera Hack Leads to Threats and Racial Slurs*, GUARDIAN (Dec. 23, 2020), https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats [https://perma.cc/9NB9-NSJ8].

227. GAO REPORT 2007, *supra* note 30, at 19.

228. *E.g.*, *In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018) (describing how 24 million Zappos users were impacted by the cyber-attack breach).

229. Twitter was founded in March of 2006. Nicholas Carlson, *The Real History of Twitter*, BUS. INSIDER (Apr. 23, 2011), https://www.businessinsider.com/how-twitter-was-founded-2011-4 [https://perma.cc/66Q5-9DWE]. This is anecdotal at best since Twitter is only one place that can be breached, but a lot has changed since 2006 in the sphere of technology. The government should grow and research and review with the pace of technological change.

230. *See, e.g.*, Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1343 (11th Cir. 2021); *In re* SuperValu, Inc., 870 F.3d 763, 771 (8th Cir. 2017).

data protection on consumers, not just through writing new legislation but funding updated research to look at the impact of the modern data life cycle. "It is possible that some years later there may be more detailed factual support [than the 2007 GAO report] for plaintiffs' allegations of future injury."[231] That time is now, and the federal government should renew efforts to study the connection between data breaches and identity theft. These studies are likely to show a substantial risk of harm from compromised data that would provide standing for many more impacted individuals than previously existed.

CONCLUSION

Data breaches have become commonplace in 2023. Consumers are paying more and more attention to what information is shared with the businesses they patronize. This personal information is still out there, and in the wrong hands it can be used by nefarious parties to steal identities. When a company gets hacked and loses consumer data, a recourse in our legal system is a civil suit against the company. The biggest issue facing many data breach victims is articulating how the data breach has harmed them in a way that creates Article III standing before there is evidence of misuse of the data. *Ramirez* creates a catch-22 by requiring an actual injury alongside the substantial risk of injury to allow for recovery of damages. This puts consumers in the murkiest of murky waters. Adopting a clear rule to define when there is a substantial risk of harm regarding data breaches is the best path forward. A data type rule focused on static PII, like Social Security Numbers, protects consumers without overburdening the courts with underbaked lawsuits.

231. *In re SuperValu*, 870 F.3d at 771.