Brooklyn Law Review

Volume 88 | Issue 3 Article 5

4-23-2023

Standing in the Age of Data Breaches: A Consumer-Friendly Framework to Pleading Future Injury and Providing Equitable Relief to Data Breach Victims

John E. McLoughlin

Standing in the Age of Data Breaches

A CONSUMER-FRIENDLY FRAMEWORK TO PLEADING FUTURE INJURY AND PROVIDING EQUITABLE RELIEF TO DATA BREACH VICTIMS

INTRODUCTION

As technology constantly develops and electronic communications and transactions become more ubiquitous, so do data breaches.[1] In 2020 alone, there were over one thousand data breaches in the United States, with data exposures affecting over 310 million Americans in the same year.[2] Unfortunately, there is no sign of those figures decreasing any time soon, as the companies that expose confidential records are allowed to continue operating with limited repercussions.[3] The world's largest corporations across various industries are subject to breaches, as companies like Microsoft expose tens of millions

---

[1] Hicham Hammouchi et al., *Digging Deeper into Data Breaches: An Explanatory Data Analysis of Hacking Breaches over Time*, 151 PROCEDIA COMPUT. SCI. 1004, 1005–06 (2019).

[2] *Cyber Crime: Number of Compromises and Victims in U.S. 2005-H1 2022*, STATISTA (Aug. 31, 2022) [hereinafter *Cyber Crime*], https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ [https://perma.cc/5C9K-P4CJ].

[3] Lance Whitney, *2020 Sees Huge Increase in Records Exposed in Data Breaches*, TECHREPUBLIC (Jan. 21, 2021, 10:50 AM), https://www.techrepublic.com/article/2020-sees-huge-increase-in-records-exposed-in-data-breaches/ [https://perma.cc/UN42-AY49]; Vernon J. Richardson et al., *Much Ado About Nothing: The (Lack of) Economic Impact of Data Privacy Breaches*, 33 J. INFO. SYS. 227, 229 (2019).

of data records year after year.[4] The sad reality has become that data breaches are a question of "when," not "if," they will occur.[5]

The COVID-19 pandemic has only increased instances of cybercrime.[6] The transition to remote work and storage of data in cloud networks has led to an over 600 percent increase in cybercrime since the beginning of the pandemic.[7] Further, as more data is saved digitally, cybercriminals continuously develop new ways to profit off of stolen personal data.[8] The average consumer is in danger now more than ever, as the volume of data breaches and the damage that cybercriminals can inflict rise hand in hand.[9] Although each state has legislation in place requiring entities to notify individuals of security breaches involving their personally identifiable information (PII)[10], there is not yet federal legislation in place addressing data breach notification.[11] This makes for a mess of data breach notification law given that there are considerable discrepancies across state

---

[4] *See* Steve Symanovich, *Microsoft Accidentally Exposed 250 Million Customer Records—What You Should Know*, LIFELOCK (Feb. 4, 2021), https://lifelock.norton.com/learn/data-breaches/microsoft-exposed-250-million-customer-records [https://perma.cc/FDW6-L26D] (explaining that over 250 million customers had their personal information exposed); Tom Spring, *Microsoft Spills 38 Million Sensitive Data Records Via Careless Power App Configs*, THREATPOST (Aug. 23, 2021, 7:18 PM), https://threatpost.com/microsoft-38-million-sensitive-records-power-app/168885/ [https://perma.cc/8R4D-LYGN]; *see also* Megan Leonhardt, *The Latest Marriott Data Breach Impacts Up to 5.2 Million People—Here's What To Do if You Were Affected*, CNBC (Mar. 31, 2020, 5:32 PM), https://www.cnbc.com/2020/03/31/what-to-do-if-you-were-affected-by-the-latest-marriott-data-breach.html [https://perma.cc/FAF7-LGG5] (explaining that 5.2 million guests at Marriott hotels had their personal data—including names, personal details, addresses, and employer information—exposed by cybercriminals).

[5] Tyler Anders et al., *Not "If" but "When"—The Ever Increasing Threat of a Data Breach in 2021*, JD SUPRA (July 15, 2021), https://www.jdsupra.com/legalnews/not-if-but-when-the-ever-increasing-8569092/ [https://perma.cc/B56R-V2B2].

[6] Ruston Miles, *You've Been Hacked. Now What?*, SEC. INFOWATCH (Sept. 7, 2021), https://www.securityinfowatch.com/cybersecurity/information-security/breach-detection/article/21237243/youve-been-hacked-now-what [https://perma.cc/UEU8-U4EA].

[7] *Id.*

[8] *Id.*; *see also* Alex Scroxton, *Data Breaches Are a Ticking Time Bomb for Consumers*, COMPUT. WKLY. (Feb. 9, 2021), https://www.computerweekly.com/news/252496079/Data-breaches-are-a-ticking-timebomb-for-consumers [https://perma.cc/CKB7-5JMM].

[9] *See* Juliana De Groot, *The History of Data Breaches*, DIGIT. GUARDIAN (Aug. 22, 2022), https://digitalguardian.com/blog/history-data-breaches [https://perma.cc/UHV7-XYBY]; *see also* Scroxton, *supra* note 8.

[10] PII is broadly defined "as any information that permits the identity of an individual to be directly or indirectly inferred . . . [including] Social Security numbers, driver's license numbers . . . financial or medical records, biometrics," and more. *What Is Personally Identifiable Information*, DEP'T HOMELAND SEC. (Dec. 8, 2021), https://www.dhs.gov/privacy-training/what-personally-identifiable-information [https://perma.cc/6HA3-BR8J].

[11] Joseph J. Lazzarotti & Joseph C. Gavejian, *State Data Breach Notification Laws: Overview of the Patchwork*, JACKSON LEWIS (Apr. 9, 2018), https://www.jacksonlewis.com/publication/state-data-breach-notification-laws-overview-patchwork [https://perma.cc/ED2T-SXPX].

lines.[12] Even more, upon being notified of a breach, consumers across the United States have limited legal options.[13]

When someone finds out that their PII has been stolen, fear is the natural reaction: fear of identity theft, financial losses, or other personal information being exploited.[14] After being notified of such a breach, individuals may seek to sue the entity that was entrusted with keeping their PII secure.[15] In many cases, however, consumers are prohibited from bringing a claim.[16]

An essential element to establish standing under Article III of the Constitution is showing "injury in fact."[17] If someone is notified of a data breach but their PII has not yet been used by a separate party, it follows that they have not yet been injured.[18] Therefore, the only legal claim that data breach victims can make if they have yet to be injured is to plead future injury as a result of the breach, which has proved to be an exceptionally high bar to meet.[19] A claim for a future injury will only be sufficient to satisfy Article III standing "if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur."[20] Most Americans who are notified of a data breach are stuck in a legal state of limbo where they know of the

---

[12] *Id.*

[13] *See Security Breach Notification Laws*, NAT'L CONF. STATE LEGS. (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/6W8B-PZ8Q]; *see generally* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-230, DATA BREACHES: RANGE OF CONSUMER RISKS HIGHLIGHTS LIMITATIONS OF IDENTITY THEFT SERVS. 12 (2019), https://www.gao.gov/assets/gao-19-230.pdf [https://perma.cc/5M89-AHME] (explaining that there is not one fix-all solution that can be taken when a data breach occurs).

[14] *See* ANNE JOHNSON & LYNETTE I. MILLETT, NAT'L ACADS. SCIS., ENG'G, & MED., DATA BREACH AFTERMATH AND RECOVERY FOR INDIVIDUALS AND INSTITUTIONS: PROCEEDINGS OF A WORKSHOP 6 (2019).

[15] *See* Margaret A. Dale & David A. Munkittrick, *Data Breach Litigation Involving Consumer Class Actions*, *in* PROSKAUER ON PRIVACY §§ 17–1, 17–2 (2d ed. 2016).

[16] *See* Devika Kornbacher et al., *No (Actual) Injury, No Problem: Second Circuit Recognizes an "Increased-Risk" Theory of Standing for Plaintiffs in Data Breach Cases*, JD SUPRA (May 27, 2021), https://www.jdsupra.com/legalnews/no-actual-injury-no-problem-second-6130990/ [https://perma.cc/BST4-MWQK].

[17] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (explaining that to establish an "injury in fact," the injury must be "concrete and particularized" and "actual or imminent, not 'conjectural' or 'hypothetical'" (internal quotation marks omitted) (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990))).

[18] *See* Kornbacher et al., *supra* note 16.

[19] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013) ("But respondents' theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'" (emphasis omitted) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990))).

[20] Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (quoting *Clapper*, 568 U.S. at 402).

breach, but lack sufficient standing to recover against the entity that leaked their data.[21]

Properly pleading future injury in data breach cases has been a contentious issue that has been handled differently across the federal circuits.[22] The Second Circuit Court of Appeals recently addressed this issue for the first time in *McMorris v. Carlos Lopez & Assocs., LLC*.[23] In *McMorris*, the court considered the standards used in other circuits to adopt a three-factor test for determining whether allegations of future injuries rise to the level of an Article III injury based on a theory of "increased risk of identity theft or fraud following the unauthorized disclosure of . . . data."[24] By adopting this test, *McMorris* put forward a framework in which a consumer could plausibly plead a claim for future injury in a data breach case, appearing to be one of the more consumer-friendly circuit court decisions to date.[25] However, even the friendliest circuit court decisions are increasingly unfavorable to consumers. *McMorris* still implemented significant restrictions on establishing standing for future injury in data breach cases and forbade recovery for expenses incurred to mitigate losses from a breach if the claim was not properly pled.[26]

Adding insult to injury, in 2021, the Supreme Court in *TransUnion LLC v. Ramirez* reached a decision on Article III standing for future injury that was more unfavorable to consumers than *McMorris*.[27] In Justice Kavanaugh's five-to-four majority decision, he resolved the issue of future injury by bluntly stating, "[n]o concrete harm, no standing."[28] In the wake of *TransUnion*, it is evident that the Supreme Court is reluctant to allow Article III standing for claims of future injury, making a definite guideline for pleading future injury more important than ever.[29]

---

[21] *See* Priscilla Fasoro, *Standing Issues in Data Breach Litigation: An Overview*, INSIDE PRIV. (Dec. 7, 2018), https://www.insideprivacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview/ [https://perma.cc/BQ5Z-5KZS].

[22] Nancy R. Thomas, *No Injury, No Data Breach Claims? Depends on the Circuit*, MORRISON FOERSTER (Sep. 17, 2020), https://www.mofo.com/resources/insights/200917-no-data-breach-claims.html [https://perma.cc/Y99Y-FS98].

[23] McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 302–05 (2d Cir. 2021).

[24] *Id.* at 301–03.

[25] *See* Alison Frankel, *In Major Ruling, 2nd Circuit Says No Circuit Split on Data Breaches and Standing*, REUTERS (Apr. 26, 2021, 4:24 PM), https://www.reuters.com/article/us-otc-databreach/in-major-ruling-2nd-circuit-says-no-circuit-split-on-data-breaches-and-standing-idUSKBN2CD2I4 [https://perma.cc/6ATP-V9VN].

[26] *See McMorris*, 995 F.3d at 303; *see also* Frankel, *supra* note 25.

[27] *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021).

[28] *Id.* at 2214.

[29] *See id.* at 2200; *see also* David Oberly, *Data Breach Class Actions: U.S. Supreme Court Decision May Tilt the Odds in Favor of Defendant Organizations*, JD

This note argues that the test used in *McMorris* needs to be modified and new federal data breach notification legislation needs to be implemented to give data breach victims a fair shot at Article III standing and a chance of recovery. More specifically, although the test introduced by *McMorris* is a step in the right direction for greater consumer protection, a revised test that is less malleable would reign in judges' broad discretion.[30] By rearranging the factors explained in *McMorris*, this new test for standing will provide equitable relief for plaintiffs bringing future injury claims. Furthermore, even with a fixed test for standing in place, the Supreme Court's 2013 ruling in *Clapper v. Amnesty Int'l USA* allows the companies responsible for data breaches to escape liability by prohibiting individuals claiming future injury from recovering for any mitigation expenses taken subsequent to a notification.[31] Therefore, this note also proposes federal data breach notification legislation—modeled after California's data breach notification legislation[32]—that includes recovery for reasonable preventative actions taken after a breach.

Part I of this note explains the background and rising prevalence of data breaches and gives a brief overview of the existing legislation for data breach security, protection, and notification. Part II gives an in-depth explanation of the *McMorris* decision as well as some of the cases that informed *McMorris*'s three-step test. This Part also explains the dangerous precedent set by the *TransUnion* decision and the bleak legal outlook it gave plaintiffs trying to bring a case of future injury. Finally, Part III proposes a solution to pleading future injury claims, including tweaking the process provided in *McMorris*, as well as implementing federal data breach notification legislation that allows for recovery of any reasonable expenses that data breach victims incur in trying to protect themselves from future injury.

SUPRA (Aug. 4, 2021), https://www.jdsupra.com/legalnews/data-breach-class-actions-u-s-supreme-5349175/ [https://perma.cc/Q63F-TGFE] ("[T]he mere risk of future harm alone is no longer sufficient to confer standing. This is particularly significant in the context of data breach class action litigations, where suits are often filed in the immediate aftermath of a cyber-attack even where no actual harm—in the form of identity theft or fraud—has yet occurred.").

[30] *See McMorris*, 995 F.3d at 303 (explaining that the list of factors in *McMorris* is "non-exhaustive").

[31] *See* Daniel Solove, *Standing in Data Breach Cases: Why Harm Is Not Manufactured*, TEACHPRIVACY (Feb. 15, 2021), https://teachprivacy.com/standing-in-data-breach-cases-why-harm-is-not-manufactured/ [https://perma.cc/WPC3-LLDS].

[32] *See* CAL. CIV. CODE § 1798.29 (West, Westlaw current with all laws through Ch. 997 of the 2022 Reg. Sess.).

I. DATA BREACHES AND THE LEGISLATION IN PLACE TO PROTECT CONSUMERS

The volume of data breaches has grown exponentially in the since the 1980s, when data breaches first started.[33] Despite increasing prevalence, the economic impacts of breaches are inconsequential for large companies, providing companies with little incentive to sufficiently safeguard against breaches.[34] Individual consumers, on the other hand, may suffer potentially debilitating injuries as the result of a breach.[35] While there are some data breach notification laws in place, these laws do not do enough to discourage data breaches for most large companies, leaving the average American consumer a sitting duck, waiting to have their PII stolen.[36]

A. The History of Data Breaches

A data breach occurs when an individual loses or suffers the theft of their "data containing sensitive personal information . . . result[ing] in the potential compromise of the confidentiality or integrity of the data."[37] Data breaches affect consumers across the world who have entrusted "[r]etailers, hospitals, corporations, government offices and colleges" with their PII.[38] A breach may result from the intentional actions of cybercriminals or from an accidental leak from the entity storing the information.[39] Following any instance of a breach, there exists the possibility that a cybercriminal may access PII and profit from that information at the consumer's expense.[40]

Data breaches began to increase in frequency in the 1980s and 90s, but the recording of the largest breaches did not begin until 2005, due largely in part to the spread of electronic data during the mid 2000s.[41] The volume of breaches and records

---

[33] *See* De Groot, *supra* note 9; *see also Cyber Crime*, *supra* note 2.

[34] *See* Richardson et al., *supra* note 3, at 227.

[35] Scroxton, *supra* note 8.

[36] *See* Richardson et al., *supra* note 3, at 249.

[37] 38 C.F.R. § 75.112 (2022) (formatting omitted).

[38] Steve Symanovich, *What Is a Data Breach and How Do I Handle One?*, LIFELOCK (July 31, 2017), https://www.lifelock.com/learn-data-breaches-data-breaches-need-to-know.html [https://perma.cc/KWU2-ZYHZ].

[39] *Id.*

[40] *Id.*

[41] *See* De Groot, *supra* note 9; *see also* Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (July 16, 2021), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/QUV2-WRVU] (explaining that the largest breach in history—Yahoo in 2013—exposed over 3 billion consumer accounts).

exposed have had upward trends ever since that time.[42] In 2020 alone, Microsoft exposed 38 million private records, just one year after it was reported that the company had exposed over 250 million records from 2005 to 2019.[43] Notably, these prolonged breaches are not out of the ordinary. For example, Marriott exposed the PII of over 300 million guests throughout the period from 2014 through 2018, providing cybercriminals with ample opportunity to steal and profit off stolen PII.[44]

Despite the upward trend in data breaches year after year, cybercriminals have more data to compromise now than ever before because of the COVID-19 pandemic.[45] A major consequence of the pandemic was the forced transition for many to work from home, and, as such, more PII began to be stored in cloud networks.[46] Additionally, workers began accessing highly secure work networks remotely from less secure home Wi-Fi networks, making PII and company data vulnerable.[47] Consequently, cybercriminals have been gifted with easy opportunities to steal PII.[48] Not only have there been more data breaches, but the average cost of a data breach—which consists of costs incurred from data breach detection and escalation, notification activities, lost business, and post-breach responses—rose from $3.86 million in 2020 to $4.24 million in 2021, the highest it has ever been.[49] Thus, the COVID-19

---

[42] *See* De Groot, *supra* note 9; *see also Cyber Crime*, *supra* note 2.

[43] Symanovich, *supra* note 4 (noting that most of the exposed information consisted of customer service and support logs although some customers may have had their email addresses exposed); Spring, *supra* note 4 (explaining that Social Security Numbers, COVID-19 vaccination statuses and email addresses were exposed).

[44] *See* Lindsey O'Donnell, *Marriott Hotel Data Breach: Ongoing Since 2014*, THREATPOST (Nov. 30, 2018), https://threatpost.com/2014-marriott-data-breach-exposed-500m-guests-impacted/139507/ [https://perma.cc/PUK2-TAB9].

[45] Miles, *supra* note 6.

[46] *Id.*

[47] *See id.*

[48] *See* Blake Dillon, *Protecting Information While Working From Home—One Year Later*, JD SUPRA (Apr. 12, 2021), https://www.jdsupra.com/legalnews/protecting-information-while-working-4868603/ [https://perma.cc/6LCN-3TRZ]; *see also* Ellen Sheng, *Cybercrime Ramps Up Amid Coronavirus Chaos, Costing Companies Billions*, CNBC (July 29, 2020, 12:00 PM), https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html [https://perma.cc/4P4A-8ZCL].

[49] IBM SEC., COST OF A DATA BREACH REP. 2021 4 (2021), https://www.ibm.com/downloads/cas/OJDVQGRY [https://perma.cc/2CQQ-KHEZ]; *see also* Tim Richardson, *Security Breaches Where Working from Home is Involved Are Costlier, Claims IBM Report*, REG. (July 28, 2021), https://www.theregister.com/2021/07/28/cost_of_a_data_breach_report_2021/ [https://perma.cc/BR8L-K7B6] (noting that the average cost of a remote working data breach is more than $1 million higher than a breach that does not involve remote work).

pandemic has penetrated and enlarged the cracks of an already weak American online infrastructure.[50]

To exacerbate the problem, cybercriminals are constantly innovating new ways in which they can profit off of stolen PII.[51] In recent years, cybercriminals have started to target health care data at a vastly increased rate, as well as digital wallets and payment methods such as Venmo, which have provided hackers with easy access to consumer credit information.[52] As new schemes become apparent, the path to becoming a cybercriminal is easier than ever.[53] Malware tools needed to steal online information are now cheaper to buy, easier to obtain, and simpler to use than they have been in the past.[54] Additionally, it has become simpler for cybercriminals to sell PII due to the emergence of Amazon-like marketplaces on the regular internet.[55]

Despite the rise of accessible marketplaces on the regular internet, The dark web has been a familiar and secure marketplace for cybercriminals to sell stolen PII, and it has not lost any traction.[56] The dark web remains the premier

---

[50] Kat Jercich, *Healthcare Data Breaches on the Rise*, HEALTHCARE IT NEWS (Aug. 5, 2021, 9:14 AM), https://www.healthcareitnews.com/news/healthcare-data-breaches-rise [https://perma.cc/YQ7Y-43YM] (Kailash Ambwani, CEO of Constella Intelligence, explained that "[t]he COVID-19 pandemic has shown us the fragility of our online infrastructure . . . As people continue to rely on digital solutions and [work] from home, both companies and individuals must take new precautions to protect themselves from potential threat actors.") (second alteration in original).

[51] *See* Davey Winder, *Revealed: The Supermarkets That Will Sell You Malware for $50*, FORBES (Apr. 28, 2020, 4:33 PM), https://www.forbes.com/sites/daveywinder/2020/04/28/revealed-the-supermarkets-that-will-sell-you-malware-for-50/ [perma.cc/P9HB-8S4D].

[52] Ravi Sen, *Here's How Much Your Personal Information Is Worth to Cybercriminals—and What They Do With It*, NEXTGOV (May 14, 2021), https://www.nextgov.com/ideas/2021/05/heres-how-much-your-personal-information-worth-cybercriminals-and-what-they-do-it/174055/ [https://perma.cc/EZU6-MPCE]; *see also* Vildan Altuglu et al., *Assessing Damages in Data Privacy and Data Breach Class Actions Involving Health Data in the Wake of COVID-19*, NAT'L L. REV. (Mar. 15, 2021), https://www.natlawreview.com/article/assessing-damages-data-privacy-and-data-breach-class-actions-involving-health-data [https://perma.cc/Q5BH-M78X]; Megan Leonhardt, *Consumers Lost $56 Billion to Identity Fraud Last Year—Here's What to Look Out For*, CNBC (Mar. 23, 2021), https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html [https://perma.cc/X3RP-B9YJ].

[53] Winder, *supra* note 51.

[54] *Id.*

[55] *See* Dan Patterson, *Inside Genesis: The Market Created by Cybercriminals to Make Millions Selling Your Digital Identity*, CBS NEWS (Sept. 9, 2021), https://www.cbsnews.com/news/genesis-cybercriminal-market-ransomware/ [https://perma.cc/85CE-68KY].

[56] *See* Beenu Arora, *Five Key Reasons Dark Web Markets are Booming*, FORBES (Apr. 23, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/04/23/five-key-reasons-dark-web-markets-are-booming/ [https://perma.cc/XP23-JQ66]; *see also* Sen, *supra* note 52. The Dark Web is defined as "the set of web pages on the World Wide Web that cannot be indexed by search engines, are not viewable in a standard Web browser, require specific means (such as specialized software or network configuration) in order

marketplace for practiced cybercriminals to sell stolen PII, and as long as cybercriminals have access to Bitcoin—a common payment method for dark web transactions—they will have no problem selling data on the Dark Web.[57] A common incentive for cybercriminals behind data breaches is the potential profit from stolen information, and the dark web offers the broadest range of buyers and the most lucrative opportunities.[58] As dark web activity rises and cybercriminals are presented with more time and resources to steal and sell information, the impact that data breaches can have on consumers continues to worsen.[59]

The overwhelming majority of information exposed in data breaches is PII.[60] A devastatingly destructive action that a cybercriminal can take with PII is identity theft, which can be accomplished through many different kinds of stolen PII and felt by victims in numerous ways such as credit fraud, medical identity theft, and criminal identity theft.[61] Additionally, if PII is sold "on the [d]ark [w]eb, it remains there indefinitely," availing cybercriminals with infinite time to steal identities and leaving victims vulnerable to the effects of identity theft years

---

to access, and use encryption to provide anonymity and privacy for users." *Dark Web*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/dark%20web [https://perma.cc/9YF5-C29S].

[57] *See* Arora, *supra* note 56; *see also* Sen, *supra* note 52.

[58] *See* Arora, *supra* note 56.

[59] *See Increased Activity Involving Stolen Data on Dark Web*, CYWARE (Oct. 27, 2021), https://cyware.com/news/increased-activity-involving-stolen-data-on-dark-web-075b0402 [https://perma.cc/9UM5-CT5V]; *see also* Taylor Schulte, *Identity Theft and Credit Card Fraud Statistics 2021*, DEFINE FIN. (July 15, 2021), https://www.definefinancial.com/blog/identity-theft-credit-card-fraud-statistics/ [https://perma.cc/VRC4-MLTD].

[60] *See* AIT News Desk, *Data Breaches Target Personally Identifiable Information in Billions of Records*, AITHORITY (June 5, 2019), https://aithority.com/security/data-breaches-target-personally-identifiable-information-in-billions-of-records/ [https://perma.cc/RPX6-Y9GJ] (citing FORGEROCK, U.S. CONSUMER DATA BREACH REP. 2019 2–4 (2019), https://www.forgerock.com/resources/view/92170441/industry-brief/us-consumer-data-breach-report.pdf [https://perma.cc/RJF5-RBRN]) (noting that "[p]ersonally identifiable information (PII) was by far the most common type of breach in 2018, representing 97% of all breaches").

[61] *See What to Know About Identity Theft*, FTC (Apr. 2021), https://www.consumer.ftc.gov/articles/what-know-about-identity-theft [https://perma.cc/2KW9-ASYQ]; *see also* Allen St. John, *Here's What Makes the Facebook Data Breach So Harmful*, CONSUMER REPS. (Oct. 12, 2018), https://www.consumerreports.org/digital-security/what-makes-the-facebook-data-breach-so-harmful-a8227559641/ [https://perma.cc/7GQU-F5B6]
(explaining that while stolen Social Security or credit card numbers cause the most damage to individual consumers, even seemingly trivial personal information can be extremely valuable to criminals); *Types of Identity Theft*, COMPLETE ID (Nov. 3 2015), https://www.completeid.com/education-center/types-of-identity-theft/
[https://perma.cc/RC4Q-J6KM]; Eugene Bekker, *What Is PII? Personally Identifiable Information*, IDENTITYFORCE (July 29, 2021), https://www.identityforce.com/blog/what-is-pii [https://perma.cc/A94Z-5Q89].

after the information is stolen.[62] In 2020 alone, Americans lost $56 billion to identity fraud, with "49 million consumers falling victim."[63] The median consumer monetary loss for identity theft is around $800, with 21 percent of victims "losing more than $20,000."[64] While the cost of a potential case of identity theft cannot be predetermined, there is a real chance that the loss will be debilitating for the average American consumer.[65]

The fastest growing type of financial crime in the United States is synthetic identity theft, which is the use of stolen PII to create and profit off of a new identity.[66] For victims of synthetic identity theft, the burden—which may include the "rejection of tax returns" or the "denial of disability benefits"—is often not felt until many years after the breach.[67] Once aware of the crime, synthetic identity theft victims must go through the arduous task of proving that they are not behind the synthetic identities in order for financial institutions to bear the majority of the financial costs.[68] However, even when financial institutions do bear the financial costs of the crime, victims still have incurred out of pocket costs such as legal fees.[69] Synthetic identity theft is expected to be an ongoing problem in the United States, as it is highly profitable for cybercriminals while simultaneously difficult for victims to detect.[70]

Obviously, there are financial consequences to identity theft and synthetic identity theft alike, but the emotional effects and loss of opportunities can sometimes be even worse for victims.[71] In a 2021 survey, identity theft victims reported increased stress levels, as they could no longer pay routine bills, and many victims reported experiencing strained relationships with their own families and friends.[72] Most concerningly, 10 percent of surveyed victims contemplated suicide after their

---

[62] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 2, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring [https://perma.cc/57K5-M5WR].

[63] Leonhardt, *supra* note 52.

[64] Schulte, *supra* note 59.

[65] *See id.*

[66] FED. RSRV., PAYMENTS FRAUD INSIGHTS JULY 2019: SYNTHETIC IDENTITY FRAUD IN THE U.S. PAYMENT SYSTEM 2–5 (2019), https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf [https://perma.cc/VTT3-W9LR] (explaining that to accomplish synthetic identity theft, cybercriminals may slightly modify stolen PII—such as a Social Security number—to create a new identity, or combine real and fake PII to form a new identity).

[67] *Id.* at 17.

[68] *Id.* at 14, 17.

[69] *Id.*

[70] *Id.* at 18.

[71] *See* IDENTITY THEFT RES. CTR., 2021 CONSUMER AFTERMATH REPORT 18 (2021).

[72] *See id.* at 6, 12, 18–19.

identity was stolen, demonstrating that the financial implications of identity theft are just the tip of the iceberg for individual consumer struggles.[73]

Despite the severe consequences of stolen PII from data breaches, in recent federal United States cases where large companies have been held liable for data breaches, the resulting settlements have been underwhelming for consumers.[74] Equifax announced that a 2017 data breach over the course of a few months exposed the PII—including Social Security numbers, birthdays, and addresses—of around 147 million people.[75] It was decided that Equifax would pay a settlement that included up to $425 million towards people affected by the breach,[76] which is a seemingly massive number to the average eye. That said, consumers affected by the breach had the option to claim "free credit monitoring services,"[77] or to opt for a cash payment.[78] "More than 4.5 million people" chose the cash payment option, yet "[o]nly $31 million of the settlement was set aside for the cash option; that works out to less than $7 a person."[79] Notably, even in cases where consumers win a settlement, their potential monetary outcome often does not come close to their potential losses from the data breach.[80]

Although the 2017 Equifax settlement is a large enough number to draw the attention of most American executives, such a large settlement is an outlier in the grand scheme of data breaches.[81] The controlling belief amongst most "executives is that 'worrying about data breaches isn't worth it.'"[82] In 2017, the average cost of a data breach was around $7.35 million per

---

[73] *See id.* at 6, 18.

[74] *See* Jody Godoy, *Equifax Data Breach Settlement Objectors Lose Appeal*, REUTERS (June 3, 2021, 6:53 PM), https://www.reuters.com/legal/litigation/equifax-data-breach-settlement-objectors-lose-appeal-2021-06-03/ [https://perma.cc/5DWZ-VY43]; *see also* George Kamel, *How a Data Breach Can Impact You*, RAMSEY (July 22, 2022), https://www.ramseysolutions.com/insurance/data-breach-impacts [https://perma.cc/2TUV-E3F4].

[75] Godoy, *supra* note 74.

[76] *Equifax Data Breach Settlement*, FTC (Sept. 2022), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement [https://perma.cc/T3S8-Z4KZ].

[77] *See* Tara Seigel Bernard, *Equifax Breach Affected 147 Million, but Most Sit Out Settlement*, N.Y. TIMES (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/business/equifax-breach-settlement.html [https://perma.cc/R7DV-T3RG] (explaining that under the "free credit monitoring" option, individuals affected by the breach could choose to receive a "free credit monitoring service[ ]" or reclaim a maximum of $125 if they already had a credit monitoring service).

[78] *See id.*

[79] *Id.*

[80] *See* Kamel, *supra* note 74.

[81] *See* Richardson et al., *supra* note 3, at 230.

[82] *Id.* at 229–30.

breached company, with extreme outliers like Equifax skewing that number upward.[83] Rather than spend tens of millions of dollars on data security measures, most executives have seen it as a better business decision to take the monetary hit from the suits resulting from the breaches that inevitably come their way.[84] While there are few significant consequences to the average company experiencing a data breach, consumers are left to bear the brunt of the harm when breaches occur.[85] Consumers are left vulnerable to the many schemes and pathways that cybercriminals have at their disposal to steal and sell PII, which makes the laws that are in place to protect consumers from data breaches increasingly important.[86]

B. Data Breach Legislation in Place

Although there are laws in place to prevent data breaches and notify consumers of breaches, the United States has taken a largely sectoral approach to data privacy laws.[87] The most relevant legislation in place for consumers is the Federal Trade Commission (FTC) Act which empowers the FTC to enforce privacy laws.[88] Under Section 5 of the FTC Act, the FTC can bring data security enforcement actions against US companies that engage in "unfair or deceptive acts or practices in or affecting commerce."[89] Still, the FTC has not enacted regulations that establish data security requirements.[90] Other important federal laws in place that govern the collection of online information include the Health Insurance Portability and

---

[83] *Id.* at 230.

[84] *See id.* at 229–30.

[85] *See id.* at 249.

[86] *See* Laurel Thomas, *Data Breaches: Most Victims Unaware When Shown Evidence of Multiple Compromised Accounts*, UNIV. OF MICH. NEWS (June 21, 2021), https://news.umich.edu/data-breaches-most-victims-unaware-when-shown-evidence-of-multiple-compromised-accounts/ [https://perma.cc/9ZYV-YUYL].

[87] Angelique Carson, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (July 20, 2021), https://www.osano.com/articles/data-privacy-laws [https://perma.cc/GH7L-NDMT] (explaining that a wide variety of sector-specific laws governed by government agencies exist, but there is not one overreaching federal law governing data privacy in the United States).

[88] Federal Trade Commission Act of 1914, Pub. L. No. 63-203, 38 Stat. 717 (codified as amended at 15 U.S.C. § 45); *see also* FED. TRADE COMM'N, FEDERAL TRADE COMMISSION 2020 PRIVACY AND DATA SECURITY UPDATE 1 (2020), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf [https://perma.cc/GDS4-2VJ2].

[89] An Act to amend creating the Federal Trade Commission, to define its powers and duties, and for other purposes, Pub. L. No. 447 § 5, 75 Stat. 717 (codified at 15 U.S.C. § 45).

[90] *FTC Data Security Standards and Enforcement*, PRAC. L. DATA PRIV. ADVISOR 1 (last visited Feb. 1, 2023), Westlaw Prac. Note 8-617-7036.

Accountability Act (HIPAA), which governs the collection of health information, the Fair Credit Reporting Act (FCRA), which regulates the use of credit information, and the Payment Card Industry Data Security Standard (PCI DSS), which provides guidelines for companies that maintain and process consumer credit card information.[91]

The most recent administrative data compliance legislation—the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)—was signed into law by President Biden in March 2022.[92] CIRCIA sets out to implement reporting requirements on specified critical infrastructure "covered entit[ies]" to inform the government about cybersecurity incidents.[93] However, CIRCIA—like other federal cybersecurity requirements—"pertain[s] to cyber[security] incident reporting rather than data[] breach [notification disclosures], which differ."[94] Whereas cybersecurity incidents "occur[] when the confidentiality [or] integrity . . . of a digital asset or its function is compromised[,] . . . 'data breach[es]' occur[] when it [has been] confirmed that data residing on an asset or system was compromised."[95] In other words, cybersecurity incidents—which CIRCIA and other administrative legislations are concerned with—may not always rise to the level of being data breaches, meaning that CIRCIA and other cybersecurity incident legislations do not address all data breaches.[96]

A positive effect of CIRCIA is that it may motivate other federal agencies to take similar actions with regards to

---

[91] Carson, *supra* note 87; *see also* Juliana De Groot, *What Is HIPAA Compliance?*, DIGIT. GUARDIAN (Apr. 4, 2022), https://digitalguardian.com/blog/what-hipaa-compliance [https://perma.cc/FT93-BM3G]; Juliana De Groot, *What is PCI Compliance?*, DIGIT. GUARDIAN (Aug. 12, 2021), https://digitalguardian.com/blog/what-pci-compliance [https://perma.cc/WZ79-WLEV]; *PCI FAQs*, PCI COMPLIANCE GUIDE, https://www.pcicomplianceguide.org/faq/#1 [https://perma.cc/P5VW-FXQC].

[92] Fran Faircloth et al., *Expansive Federal Breach Reporting Requirement Becomes Law*, ROPES & GRAY LLP (Mar. 22, 2022), https://www.ropesgray.com/en/newsroom/alerts/2022/March/Expansive-Federal-Breach-Reporting-Requirement-Becomes-Law [https://perma.cc/5FW4-W87X].

[93] Michael T. Borgia, *The Cyber Incident Reporting for Critical Infrastructure Act of 2022: An Overview*, DAVIS WRIGHT TREMAINE LLP (May 18, 2022), https://www.dwt.com/blogs/privacy—security-law-blog/2022/05/cyber-incident-reporting-act-2022 [https://perma.cc/6K5B-7DP3].

[94] Sofia Lesmes & Mary Brooks, *By the Numbers: Parsing Cybersecurity Incident and Breach Reporting Requirements*, R STREET (Sept. 1, 2022), https://www.rstreet.org/2022/09/01/by-the-numbers-parsing-cybersecurity-incident-and-breach-reporting-requirements/ [https://perma.cc/RG23-33WG].

[95] *Id.*

[96] *Id.*

cybersecurity legislation.[97] Notably, in January 2023, the Federal Communications Commission (FCC) proposed a rule that would strengthen data breach notification requirements for telecommunication companies.[98] If adopted, the new rule would eliminate the mandatory seven-day period that telecommunication companies must wait before they can notify customers of a data breach.[99] Thus, under the FCC's proposed rule, individuals could take action to protect their breached information immediately after a breach rather than wait seven days, lessening the potential impact of the breach on those individuals.[100] Although the FCC's proposed rule is a step in the right direction for consumers, and despite the many agency data compliance regulations that are in place or on the horizon, there is not yet federal data breach notification legislation, leaving state legislatures to enact their own data breach notification laws.[101]

All fifty states have enacted their own data breach notification laws and there are common threads to the different state laws, including provisions that require immediate action to contain a breach, "[n]otification to . . . state residents without unreasonable delay," and civil penalties enforced by state attorney generals.[102] Nonetheless, the notification law requirements in different states vary, sometimes drastically, making the current approach to data breach notification law a confusing patchwork of state law.[103] For instance, while a number of states have recently been cracking down on notification timelines,[104] there is still great disparity with respect to notification timelines across state laws, with some states being much tougher than others.[105] Alabama, for example, has rather loose laws in place, where "[i]f, after a good faith investigation, it's determined that there is not likely a

---

[97] *See* Alicia Hope, *FCC Introduces New Data Breach Notification Rules for Telecommunications Companies*, CPO MAG. (Jan. 17, 2023), https://www.cpomagazine.com/cyber-security/fcc-introduces-new-data-breach-notification-rules-for-telecommunications-companies/ [https://perma.cc/B9PQ-3ZR3].

[98] *See* Data Breach Reporting Requirements, 88 Fed. Reg. 14, 3953 (Jan. 23, 2023).

[99] *Id.*

[100] *See id*; *see also* Hope, *supra* note 97.

[101] *See* Lazzarotti & Gavejian, *supra* note 11.

[102] *See* DIGIT. GUARDIAN, THE DEFINITIVE GUIDE TO US STATE DATA BREACH LAWS 1 (2019), https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf [https://perma.cc/N3NP-Y2EB]; *see also* Lazzarotti & Gavejian, *supra* note 11.

[103] *Id.*

[104] Michael T. Borgia et al., *Multiple States Toughen Data Breach and Cybersecurity Requirements*, DAVIS WRIGHT TREMAINE (Aug. 12, 2021), https://www.dwt.com/blogs/privacy—security-law-blog/2021/08/new-state-data-breach-laws-2021 [https://perma.cc/Y8LP-X58R].

[105] DIGIT. GUARDIAN, *supra* note 102, at 1.

substantial risk of harm, notification is not required."[106] California, on the other hand, does not allow for any analysis of the risk of harm, requiring notification in every instance of a breach.[107] Across the board, state notification statutes have a variety of different definitions of "personal information" and "breach," as well as differing analyses of risk of harm and notification timing requirements.[108]

Europe, on the other hand, recently enacted "the toughest privacy and security law in the world"—the General Data Protection Regulation (GDPR)—that "imposes heavy fines against those who violate its privacy and security standards (which are quite broad)."[109] Some US states have tried to follow in Europe's footsteps. The California Consumer Privacy Act—one part of California's "larger legal framework that regulates the collection . . . and disclosure of personal information . . . in conjunction with" California's data breach notification legislation and the California Privacy Rights Act—was the first state action to mirror some aspects of the GDPR.[110] While a handful of other states have followed in California's footsteps,[111] no two state laws are the same, and none come close to the stringency of the GDPR.[112]

II. AN ANALYSIS OF *MCMORRIS* AND RELEVANT CASES

As the number of data breaches continues to rise, so does the number of lawsuits filed after every reported breach.[113]

---

[106] *Id.* at 2–4.

[107] FOLEY & LARDNER LLP, STATE DATA BREACH NOTIFICATION LAWS 9–10 (2020), https://www.foley.com/en/insights/publications/2019/01/-/media/files/insights/publications/2020/04/20mc28174-data-breach-chart-041720.pdf [https://perma.cc/GF7D-PE7B].

[108] *See generally id* at 23, 35 (For example, Illinois defines "breach" as "[u]nauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector." Alternatively, Massachusetts defines "breach" as "[u]nauthorized acquisition or unauthorized use of unencrypted data or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident.").

[109] Bryan Clark, *GDPR in the USA? New State Legislation Is Making This Closer to Reality*, NAT'L L. REV. (Mar. 18, 2021), https://www.natlawreview.com/article/gdpr-usa-new-state-legislation-making-closer-to-reality [https://perma.cc/EDE4-AMU4].

[110] *Id*; *see also A New Standard for Data Breach Laws in the U.S.*, CASEGUARD (Mar. 22, 2022), https://caseguard.com/articles/a-new-standard-for-data-breach-laws-in-the-u-s [https://perma.cc/9ECL-MLKC].

[111] *See*, *e.g.*, VA. CODE ANN. § 59.1-578 (West, Westlaw current through the 2023 Reg. Sess. cc. 1 to 3).

[112] *See generally* Clark, *supra* note 109 (outlining the new and proposed privacy laws in the US).

[113] *See* Dale & Munkittrick, *supra* note 15, at 1–2.

However, a problem that claimants may face is meeting the constitutional barrier of having been "injured in fact."[114] Individuals who are notified of a breach may have either not yet been injured or may not yet be aware of an injury that they have already suffered.[115] Given that data breaches did not become a significant problem until the turn of the twenty-first century, the legal landscape for pleading future injury in data breach cases is constantly changing and evolving.[116] That said, *McMorris v. Carlos Lopez* built on factors discussed in sister circuits to establish a framework for victims of data breaches to plead future injury.[117] *McMorris*, however, is not without its flaws, and in the wake of *TransUnion LLC v. Ramirez*, claimants of future injury could be left in the dark.[118]

A. A History of Article III Standing Decisions

Despite the Constitution being written over two hundred years ago, our current understanding of Article III standing requisites were not made clear until the Supreme Court decision of *Lujan v. Defenders of Wildlife* in 1992.[119] In *Lujan*, Justice Scalia introduced the "constitutional minimum of" three elements to establish Article III standing: (1) "injury in fact," (2) "a causal connection between the injury and the conduct complained of," and (3) a likelihood "that the injury will be 'redressed by a favorable decision.'"[120] The first element—injury in fact—is the barrier faced by claimants for future injury.[121] Justice Scalia's landmark opinion defined injury in fact as "a concrete and particularized, actual or imminent invasion of a legally protected interest."[122] In data breach claims in particular, the "legally protected interest" that victims often claim to be invaded is the fundamental right of privacy.[123]

Scalia cited *Marbury v. Madison* to justify his opinion that to ignore the concrete injury requirement would be to discard the fundamental role of the judicial branch "to decide on

---

[114] Kornbacher et al., *supra* note 16.

[115] *See* Fasoro, *supra* note 21.

[116] *See id.*

[117] McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301–03 (2d Cir. 2021).

[118] *See* Oberly, *supra* note 29; *infra* Section II.C.

[119] *See* Max Kennerly, *Rethinking Article III Standing Requirements*, LITIG. & TRIAL (Feb. 8, 2017), https://www.litigationandtrial.com/2017/02/articles/attorney/standing/ [https://perma.cc/LD8K-634P].

[120] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992) (citations omitted) (quoting Simon v. Eastern Kentucky Welfare Rts. Org., 426 U.S. 26 (1976)).

[121] Kornbacher et al., *supra* note 16.

[122] *Lujan*, 504 U.S. at 555.

[123] *See* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301 n.3 (2d Cir. 2021).

the rights of individuals."[124] Justice Blackmun's dissent in *Lujan*, however, used *Marbury* to make an opposite argument: courts owe substantial deference to Congress' purpose of imposing certain procedural requirements.[125] Nonetheless, post-*Lujan*, courts have been bound by Justice Scalia's judicially created doctrine of standing, resulting in a confused understanding of Article III standing that has been interpreted differently by lower courts.[126]

Throughout the 2010s, courts attempted to interpret the language used in the *Lujan* decision but struggled to find commonality in those interpretations. In *Clapper v. Amnesty Int'l USA*, plaintiffs pleading future injury for unconstitutional surveillance under the Foreign Intelligence Surveillance Act were denied standing as the court focused on the idea that the pleaded injury must be "certainly impending."[127] *Clapper* declared that plaintiffs "cannot manufacture standing . . . based on hypothetical future harm[s]."[128] However, *Susan B. Anthony List v. Driehaus* later provided a glimmer of hope for claimants of future injury, as the decision explained that the injury could be "'certainly impending,' or there [be] a 'substantial risk' that the harm will occur."[129] The *Driehaus* decision ruled in favor of the claimants for future injury who proved that there was "a 'substantial risk' that the harm will occur," on the basis that there had been proof of real injury from the same conduct in the past.[130]

Later, in *Spokeo, Inc. v. Robins*, a case that involved the inaccurate reporting of files under the FCRA, the Court remanded because the circuit court did not "appreciate the distinction between concreteness and particularization."[131] The Court ruled that the injury pleaded in *Spokeo*—a procedural violation under the FCRA—was not proven to be "concrete" or "actually exist[ing]," because the bare procedural violation in the case could have resulted in no harm at all.[132] Rather than approach the standing issue head on, the *Spokeo* court declined to make any judgement on the question of standing and remanded it for further consideration, highlighting the tentative

---

[124] *Lujan*, 504 U.S. at 576 (quoting Marbury v. Madison, 5 U.S. 137, 170 (1803)).
[125] *Id.* at 606 (1992) (Blackmun, J., dissenting).
[126] Kennerly, *supra* note 119.
[127] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401–02 (2013).
[128] *Id.* at 402.
[129] Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014).
[130] *Id.* at 158, 164.
[131] Spokeo, Inc. v. Robins, 578 U.S. 330, 342 (2016).
[132] *Id.* at 342–43.

and uncertain approach that courts take when it comes to pleadings of future injury.[133]

Although consequential for pleading Article III standing, none of the aforementioned cases from the 2010s dealt with data breaches. The first circuit court decision involving future injury for a data breach was the Seventh Circuit decision of *Pisciotta v. Old National Bancorp* in 2007.[134] *Pisciotta* introduced the Seventh Circuit's recognition that the injury in fact requirement can be fulfilled by the threat or increased risk of future harm.[135] In the years since *Pisciotta*, data breach decisions in the Sixth, Ninth, and DC Circuits have joined the Seventh Circuit in recognizing that plaintiffs can establish standing based on a risk of future injury.[136] The most recent of these decisions was the 2019 DC Circuit decision of *In re U.S. Office of Personnel Management Data Security Breach Litigation*.[137] In finding that the hackers in this case had both the ability and intent to use breached data for ill against plaintiffs, the court held that there was an increased risk of injury and granted the plaintiff Article III standing.[138]

Contrastingly, the Second, Third, Fourth, Eighth, and, most recently, Eleventh Circuits have not recognized standing based on a theory of increased risk of future injury in data breach cases.[139] Indeed, certain circuit courts have spent more time and effort interpreting future injury than others, which has led many to believe that a circuit split exists on the issue.[140] As noted in *McMorris*, however, even those decisions declining to find standing have not "explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft."[141] Although the *McMorris* decision declared that there was not a circuit split on the issue,[142] it can be a difficult task for plaintiffs

---

[133] *Id.* at 1550 ("We take no position as to whether the Ninth Circuit's ultimate conclusion—that Robins adequately alleged an injury in fact—was correct."); *see also* Kennerly, *supra* note 119.

[134] Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 635 (7th Cir. 2007).

[135] *Id.* at 634.

[136] Kornbacher et al., *supra* note 16; *see* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010); Attias v. Carefirst, Inc., 865 F.3d 620, 627–29 (D.C. Cir. 2017).

[137] *In re* U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42 (D.C. Cir. 2019).

[138] *Id.* at 56, 59, 61, 75.

[139] Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1340, 1345 (11th Cir. 2021).

[140] *See* Kornbacher et al., *supra* note 16.

[141] McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 300 (2d Cir. 2021).

[142] *Id.* (acknowledging that "[s]ome courts have suggested that there is a circuit split on the issue," but then declaring that "no court of appeals," including those that did not find standing for plaintiffs claiming future harm, "has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft").

to establish standing even in those circuit courts that have acknowledged increased risk of future injury.[143]

B. McMorris v. Carlos Lopez & Associates

McMorris involved an email sent out to sixty-five current employees at Carlos Lopez & Associates, LLC (Carlos Lopez), containing the sensitive PII of more than one hundred past and current employees.[144] The PII shared consisted of "Social Security numbers, home addresses, dates of birth, telephone numbers, educational degrees, and dates of hire."[145] Carlos Lopez waited two weeks to address the email with its current employees but never contacted the former employees about the breach or took corrective action.[146] McMorris and two other former employees whose PII was leaked initially brought suit, and after the district court found that the plaintiffs lacked Article III standing, McMorris appealed.[147]

Taking factors utilized by other circuit courts, the Second Circuit implemented a three-step process to determine whether or not a plaintiff has properly alleged an injury:

> (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.[148]

On its face, it appears that the *McMorris* test provides victims of data breaches with clear guidelines to establish standing for future injury.[149] However, even with the "increased risk" theory implemented in the *McMorris* decision, the court found that the case was "a relatively straightforward situation" where plaintiffs did not show "a substantial risk of future identity theft or fraud."[150] In applying the three-step process, the decision acknowledged that only the third element—the

---

[143] *See* Kornbacher et al., *supra* note 16 (explaining the factor test the Second Circuit Court of Appeals applied to ultimately dismiss the case for lack of standing, even while acknowledging that "a substantial risk of future identity theft or fraud" *may* allow a plaintiff to establish standing).

[144] To be exact, the PII of 130 past and current employees was contained in these emails. *McMorris*, 995 F.3d at 298.

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.* at 303.

[149] *See id.*

[150] *Id.*

sensitivity of the data exposed—was met.[151] Accordingly, the court held that meeting the third element was not enough to establish future injury on its own.[152] In its reasoning, the court relied on *Clapper*, explaining that "[t]o [rule] otherwise would allow plaintiffs to" come up with an endless "'chain of possibilities' resulting in injury."[153]

Given that the plaintiffs in *McMorris* just barely met one of the three factors laid out in the case,[154] it is unclear how the *McMorris* factors will be weighed against each other long-term. In fact, cases since *McMorris* have applied the factors inconsistently.[155] Although *McMorris* notes that the first factor—whether or not the breach is a targeted attack—is the most important element to consider, the analysis stops there, failing to offer further insight about how heavily each factor should be weighed.[156] Additionally, the door remains open for other important factors to be added in future cases, as the decision calls the list of factors "non-exhaustive," acknowledging that determining the plaintiff's standing is fact specific.[157] While the three factors introduced by *McMorris* are the most consistently addressed in data breach cases, they "are by no means the only . . . relevant [factors]."[158]

C. McMorris*'s Preclusion of Recovery for Preventative Measures*

In addition to introducing its three-factor test, *McMorris* relied on *Clapper* to make another—possibly even more damning—ruling forbidding recovery for any expenses incurred if a future injury is not properly pled.[159] Specifically, *McMorris* ruled that where there is no proper standing for future injury, the costs plaintiffs spent mitigating the risks of future identity theft cannot be recovered, further discouraging potential data breach victims from bringing suits.[160] Data breach decisions

---

[151] *Id.* at 303–04.

[152] *Id.* at 304.

[153] *Id.* (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013)).

[154] *Id.*

[155] *See* Cotter v. Checkers Drive-In Restaurants, Inc., No. 8:19-CV-1386-VMC-CPT, 2021 WL 3773414, at *6; *see also* Cooper v. Bonobos, Inc., No. 21-CV-854 (JMF), 2022 WL 170622, at *3–4 (S.D.N.Y. Jan. 19, 2022).

[156] *McMorris*, 995 F.3d at 301.

[157] *Id.* at 303–04.

[158] *Id.* at 302.

[159] *Id.* at 303 ("[P]laintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'") (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013)).

[160] *See McMorris*, 995 F.3d at 303.

before *McMorris* also relied on *Clapper* in ruling that plaintiffs cannot create an injury based on the time and money spent protecting themselves from that "speculative threat."[161]

For example, in *Tsao v. Captiva MVP Restaurant Partners*, a targeted data breach left customers' credit card and other financial information available to hackers for nearly a full year.[162] In both *Tsao* and *McMorris*, the plaintiffs spent valuable time and money taking precautions, such as cancelling credit cards and purchasing identity theft protection services, after they were given reason to believe that their PII may have been accessed by outside third parties.[163] However, in both cases, the courts decided that the plaintiffs were merely protecting themselves from "speculative threat[s]," and were forbidden from recovering any of their reasonable expenses.[164]

Courts have used plaintiffs' appropriate preventative measures as a basis to deny them standing in data breach cases.[165] In the 2017 Second Circuit decision of *Whalen v. Michael Stores, Inc.*, after being notified of a possible data breach and taking efforts to cancel her credit card, the plaintiff brought a claim for increased risk of future identity fraud.[166] However, it was ruled that she could not have possibly "face[d] a threat of future fraud[] because her stolen credit card was promptly canceled after the breach."[167] Similarly, in *Tsao*, the court ruled that because the plaintiff immediately made efforts to cancel his cards, the risk of future fraud was effectively eliminated.[168]

McMorris explained that where plaintiffs have not "shown a substantial risk of future identity theft or fraud, 'any expenses they have reasonably incurred to mitigate that risk'" cannot create injury.[169] *McMorris* further clarified that if there is a showing of future risk of fraud, those expenses do qualify as injury in fact.[170] *McMorris*'s ruling, however, puts into question the reasoning used by the courts in *Whalen* and *Tsao*, as in those cases the court reasoned that the protective actions taken by victims was evidence that there was not a substantial risk of

---

161 *Id.*; *see also Clapper*, 568 U.S. 398, 399 ("[R]espondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending.").

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

163 *Id.*; *McMorris*, 995 F.3d at 298.

164 *Tsao*, 986 F.3d at 1334; *McMorris*, 995 F.3d at 303.

165 *McMorris*, 995 F.3d at 303.

166 Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).

167 *Id.*

168 *Tsao*, 986 F.3d at 1344.

169 *McMorris*, 995 F.3d at 303.

170 *Id.*

future harm.[171] The *Whalen* and *Tsao* courts explained that the effective mitigation steps that were taken proved that there was no risk of future injury in those cases when it was actually the risk of future injury that led to the mitigating expenses being taken in the first place.[172] This sort of circular reasoning creates a loophole for data breach defendants because if plaintiffs take reasonable mitigation efforts after a breach that extinguishes the chances of future identity theft, defendants can point to those actions as a way of proving a lack of standing.[173]

D. TransUnion LLC v. Ramirez

As the *McMorris* decision arrived, *TransUnion* was looming in the background, with the final decision coming from the Supreme Court just two months after *McMorris*.[174] Unlike the facts of *McMorris*, however, the majority of the members of the class action in *TransUnion* had yet to actually have their information be disclosed to third parties.[175] In *TransUnion*, over eight thousand individuals claimed that their credit reports were filed containing inaccurate or misleading information indicating that they were potential "terrorists, drug traffickers, or other serious criminals."[176] Less than two thousand of those individuals had their misleading reports provided to third parties.[177]

Justice Kavanaugh's decision relied heavily on *Spokeo's* requirement of a "concrete injury," and provided no standing or chance of recovery for any plaintiff who had not felt a concrete harm.[178] Kavanaugh declared that "there is a significant difference between" actual harms that are not yet quantifiable and "mere risk[s] of future harm."[179] The decision explained that pleading libel and slander, as it was pleaded in *Spokeo*, are claims of actual—but not yet quantifiable—harms, whereas pleading the future misuse of credit files is merely a risk of harm.[180] While the court reasoned that PII disclosure to third

---

171 *Whalen*, 689 F. App'x at 90; *Tsao*, 986 F.3d at 1344–45.

172 *See Whalen*, 689 F. App'x at 90; *see also Tsao*, 986 F.3d at 1344.

173 *See Whalen*, 689 F. App'x at 90; *see also Tsao*, 986 F.3d at 1344.

174 TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2190 (2021).

175 *Id.* at 2200.

176 *Id.* at 2201–03.

177 *Id.* at 2200.

178 *See id.* at 2210, 2214. Although, the decision does acknowledge that a risk of future harm can qualify as a concrete harm if "the exposure to the risk of future harm itself causes a separate concrete harm." *Id.* at 2211 (emphasis omitted). For example, a "risk of future physical, monetary, or reputational harm could cause its own current emotional or psychological harm." *Id.* at n.7.

179 *Id.* at 2211.

180 *Id.*

parties warranted standing because such a harm is similar to that associated with the tort of defamation, Justice Kavanaugh did not attempt to further explain the difference between nonquantifiable actual harms and mere risks of future harm.[181] Thus, it is unclear what other harms could be put in the category of actual, but nonquantifiable in the future.[182]

Although *TransUnion* set a dangerous precedent for pleading future injury, it was a highly contentious five-to-four decision.[183] Justice Thomas, a long-time advocate for granting standing in claims of future injury, offered his own strong dissent.[184] Justice Thomas argued that a violation of a private right—a right that every citizen is entitled to—is always "enough to create a case or controversy."[185] Thomas has introduced this private rights argument in many Article III standing cases in the past, providing a beacon of hope for plaintiffs pleading future injury.[186] In finding that TransUnion breached duties created by statute, Thomas declared that private rights were violated in this case, and as such, each class member should have standing.[187]

Thomas also introduced a common sense approach to standing in *TransUnion*, reasoning that "one need only tap into common sense to know that receiving a letter identifying you as a potential drug trafficker or terrorist is harmful."[188] While no other Supreme Court Justice signed on with Thomas's private rights approach, the other dissenting Justices in *TransUnion* built on the common sense approach to decide whether there was an actual risk of future harm.[189] Where the majority ruled that

---

[181] *Id.* at 2208–09, 2211.

[182] *See id.*

[183] *Id.* at 2191.

[184] *See id.* at 2214 (Thomas, J., dissenting); Alison Frankel, *Unlikely Bedfellows in TransUnion SCOTUS Case: Justice Thomas and Class Action Fans*, REUTERS (Mar. 11, 2021, 6:07 PM) [hereinafter *Unlikely Bedfellows*], https://www.reuters.com/article/us-otc-transunion/unlikely-bedfellows-in-transunion-scotus-case-justice-thomas-and-class-action-fans-idUSKBN2B333L [https://perma.cc/WV9E-9FKC]; *see also* Alison Frankel, *Justice Thomas' Reframing of Article III Standing is Catching on in Circuit Courts*, REUTERS (May 12, 2021, 4:26 PM) [hereinafter *Justice Thomas' Reframing*], https://www.reuters.com/business/legal/justice-thomas-reframing-article-iii-standing-is-catching-circuit-courts-2021-05-12/ [https://perma.cc/M8KE-EGM7].

[185] *TransUnion*, 141 S. Ct. at 2218 (Thomas, J., dissenting).

[186] *See Unlikely Bedfellows*, *supra* note 184; *see also, e.g.*, Thole v. U.S. Bank N.A., 140 S. Ct. 1615, 1623 (2020) (Thomas, J., concurring); Spokeo, Inc. v. Robins, 578 U.S. 330, 344–45 (2016) (Thomas, J., concurring).

[187] *TransUnion*, 141 S. Ct. at 2218 (Thomas, J., dissenting); *see also Justice Thomas' Reframing*, *supra* note 184 (noting that Samuel Issacharoff, the attorney who represented Ramirez, argued to the Justices that the class members would easily meet Thomas's standing requirements).

[188] *TransUnion*, 141 S. Ct. at 2223 (Thomas, J., dissenting).

[189] *See id.* at 2225 (Kagan, J., dissenting).

the risk of the spread of credit information to third parties was too speculative, Justice Kagan's dissent asked, "why is it so speculative that a company in the business of selling credit reports to third parties will in fact sell a credit report to a third party?"[190] Additionally, Kagan's dissent explained that "Congress is better suited than courts to" make decisions on whether something might cause a risk of harm, admitting that judges should not be seen as the end all be all of assessing real world risks of harm.[191] Despite these arguments made in the *TransUnion* dissents, issues such as inconsistent grants of standing could arise if legislation for Article III standing purposes was implemented or a common sense test for Article III standing was adopted.[192]

E. *Post*-TransUnion

After *TransUnion*, many lower courts have cited the decision "in recognition of the higher hurdle that the decision places on those future risk plaintiffs" and have dismissed cases for lack of standing.[193] Notably, however, in data breach cases post-*TransUnion*, courts have thus far managed to distinguish *TransUnion* and instead apply the *McMorris* test.[194] Some decisions have differentiated *TransUnion* procedurally, noting that at the pleadings stage it is only fair that claims of future harm be sufficient prior to any discovery being made.[195] Other data breach decisions have bypassed *TransUnion* altogether and gone straight into applying the *McMorris* test.[196] Although *TransUnion* may appear to supersede the *McMorris* test, many lower courts continue to apply *McMorris* and have noted that it is ultimately up to the Second Circuit to determine if *McMorris* has

---

[190] *See id.*

[191] *Id.* at 2226 ("Overriding an authorization to sue is appropriate when but only when Congress could not reasonably have thought that a suit will contribute to compensating or preventing the harm at issue.").

[192] *See infra* Section III.B.

[193] Molly McGinnis Stine & Tara Trifon, *Business as Usual—so Far—for Data Breach Cases After* TransUnion LLC v. Ramirez, JD SUPRA (Oct. 6, 2021), https://www.jdsupra.com/legalnews/business-as-usual-so-far-for-data-1312599/#4 [https://perma.cc/WDD6-BM7Y].

[194] *Id.*

[195] *See, e.g.*, *In re* Blackbaud, Inc., Customer Data Breach Litig., No. 3:20-MN-02972-JMC, 2021 WL 2718439, at *6 n.15 (D.S.C. July 1, 2021) (citing *Transunion*, 141 S. Ct. at 2212) ("Plaintiffs should have the benefit of discovery before being required to 'factually establish' their injuries."); *see also* Cotter v. Checkers Drive-In Restaurants, Inc., No. 8:19-CV-1386-VMC-CPT, 2021 WL 3773414, at *4 (M.D. Fla., Aug. 25, 2021).

[196] *See In re* GE/CBPS Data Breach Litig., No. 20 CIV. 2903 (KPF), 2021 WL 3406374, at *5–6 (S.D.N.Y. Aug. 4, 2021).

been overturned.[197] So far, the *TransUnion* decision has yet to spell the end for data breach future injury claimants, but it is too early to tell how these cases will be handled in the long-run.[198]

Nonetheless, as courts continue to put the *McMorris* test to use, its limitations and underdeveloped approach have only been highlighted.[199] In *In re GE/CBPS Data Breach Litig.*, plaintiffs who had their PII accessed by an unauthorized third party as the result of an email account breach were deemed to have met the first two factors of the *McMorris* test and were granted standing.[200] In *Cotter v. Checkers Drive-In Restaurants, Inc.*, plaintiffs alleged that hackers used malware to steal copies of Checkers customers' payment card data and other PII, and the plaintiffs were granted standing upon meeting only the second factor of the *McMorris* test.[201] However, in *Cooper v. Bonobos*, a plaintiff bought clothes online through Bonobos' website and years later, after hackers accessed Bonobos' cloud backup database, the plaintiff's personal information became accessible to third parties.[202] Although the case noted that the plaintiff met the first factor of the *McMorris* test, standing was not granted after it was found that the second and third factors of the test were not met.[203] Similarly, in *In re Practicefirst Data Breach Litigation*, plaintiffs were not granted standing after only meeting the third factor of the *McMorris* test.[204] Given the confusing discrepancies in court decisions regarding standing in data breach cases since *McMorris*, it is clear that the *McMorris* test is still a rough draft—its factors and their respective weights are not clearly defined.[205]

No court has provided guidance on how many of the *McMorris* factors need to be met in order to establish standing.[206]

---

[197] Alexander Bilus & Erik VanderWeyden, *After TransUnion, Lower Courts Grapple with Article III Standing in Data Breach Lawsuits*, JD SUPRA (Feb. 16, 2022), https://www.jdsupra.com/legalnews/after-transunion-lower-courts-grapple-5914252/ [https://perma.cc/SC9S-4N6W].

[198] McGinnis Stine & Trifon, *supra* note 193.

[199] *In re GE/CBPS Data Breach Litig.*, 2021 WL 3406374, at *6 (explaining that the plaintiffs met the first two factors in the McMorris test); *Cotter*, 2021 WL 3773414, at *5 (explaining that the plaintiffs met the second factors in the *McMorris* test, and gave them standing solely from that factor).

[200] *In re GE/CBPS Data Breach Litig.*, 2021 WL 3406374, at *6.

[201] *Cotter*, 2021 WL 3773414, at *5.

[202] Cooper v. Bonobos, Inc., No. 21-CV-854 (JMF), 2022 WL 170622, at *1 (S.D.N.Y. Jan. 19, 2022).

[203] *Id.* at *3–4.

[204] *In re* Practice First Data Breach Litig., No. 1:21-CV-00790 (JLS) (MJR), 2022 WL 354544, at *6 (W.D.N.Y. Feb. 2, 2022).

[205] *See* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 303 (2d Cir. 2021) (explaining that the list of factors is "non-exhaustive").

[206] *See id.* at 301; *see also Cotter*, 2021 WL 3773414, at *4–6.

Plaintiffs Cotter, Cooper, and McMorris each met one factor in their respective cases, yet Cotter was granted standing while Cooper and McMorris were not.[207] Further, in *Cotter* the plaintiff was allowed standing when only the second *McMorris* factor was met, while in *Cooper* the plaintiff was denied standing when only the first factor was met, even though the *McMorris* case itself acknowledged that the first factor is the most important to consider.[208] With the *McMorris* factors and their meanings still unclear, and *TransUnion* highlighting the current Supreme Court majority's grim outlook on future injury claims, it is time to set a clear test for standing in data breach cases.[209] Furthermore, *McMorris*'s preclusion of recovery for preventative measures disallows data breach victims who are not granted standing from recovering mitigation expenses, making it imperative that actions are taken to ensure that consumers can recover for mitigation expenses.[210]

III. MODIFYING *MCMORRIS* AND ADOPTING NEW FEDERAL DATA BREACH NOTIFICATION LEGISLATION

As *TransUnion* sets a dangerous standard, it appears as though the more favorable *McMorris* test will guide the issue of future injury standing in data breach cases for at least the considerable future.[211] Although a solid starting framework, if used as the standard test, *McMorris* could lead to unjust decisions of standing, and thus its current list of factors needs to be reworked.[212] The *McMorris* test should be modified to grant standing when it is found that breached data is sensitive such that there is an increased risk of future identity theft or fraud, in addition to any one of the following three factors: (1) "the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data," (2) "any portion of the dataset has already been misused," or (3) the data has been exposed for an excessive period of time as determined by the court on a case-by-case basis.[213] Even with a reworked *McMorris* framework, however, plaintiffs who are not granted standing will still have no way to recover from any reasonable expenses taken to

---

[207] *See Cotter*, 2021 WL 3773414, at *5; *Cooper*, 2022 WL 170622, at *3; *McMorris*, 995 F.3d at 303.

[208] *Cotter*, 2021 WL 3773414, at *5–6; *Cooper*, 2022 WL 170622, at *3–4; *McMorris*, 995 F.3d at 301.

[209] *See* Oberly, *supra* note 29.

[210] *See McMorris*, 995 F.3d at 301.

[211] *See* McGinnis Stine & Trifon, *supra* note 193.

[212] *See McMorris*, 995 F.3d at 303–04.

[213] *See id.* at 303 (explaining the three factors introduced in the decision).

mitigate the risk of future injury.[214] Therefore, the modified *McMorris* test must be implemented in addition to separate federal data breach notification legislation that allows for recovery of reasonable expenses incurred in mitigating the risk of harm. This solution will not only provide consumers with an equitable path to standing, but it will also ensure that the entities responsible for data breaches will be held accountable.[215]

A. Inequities of the Current McMorris *Test*

If there is one certainty about the issue of future injury standing, it is that judges have widely different interpretations about what amounts to injury and what does not.[216] While the current *McMorris* test provides a guideline for data breach claimants, if kept as is, judges are afforded broad discretion to give any amount of weight to each of the three *McMorris* factors, as they did in *Cooper* and *Cotter*.[217] Additionally, because *McMorris* describes its factors as "non-exhaustive," judges could base their decisions on any new factors that they come up with on a case-by-case basis.[218] If the *TransUnion* decision is any implication, there are many conflicting opinions about what kind of harm is too speculative, and if left with a malleable test like *McMorris*, decision makers would have a great deal of discretion to offer their own interpretations.[219]

Additionally, while *McMorris* and *TransUnion* were both federal cases, in their wake, the inequity of standing decisions could expand across state courts.[220] In his *TransUnion* dissent, Justice Thomas explained that the "decision [could] actually be a pyrrhic victory for" defendants attempting to dismiss cases for lack of Article III standing.[221] Post-*TransUnion*, consumer

---

[214] *See id.* at 301.

[215] *See id.* at 298; *see also* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017); Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1344 (11th Cir. 2021).

[216] *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2205–06 (2021).

[217] *McMorris*, 995 F.3d at 301, 303 (noting that the first factor is most important); Cooper v. Bonobos, Inc., No. 21-CV-854 (JMF), 2022 WL 170622, at *3 (S.D.N.Y. Jan. 19, 2022) (explaining that the plaintiffs met only the first factor in the *McMorris* test and were not granted standing); Cotter v. Checkers Drive-In Rests., Inc., No. 8:19-CV-1386-VMC-CPT, 2021 WL 3773414, at *5–6 (M.D. Fla., Aug. 25, 2021) (noting that the plaintiffs met the second factor in the *McMorris* test, and were granted standing solely from that factor).

[218] *McMorris*, 995 F.3d at 303–04.

[219] *See id.*

[220] *TransUnion*, 141 S. Ct. at 2224 n.9 (Thomas, J., dissenting); *see also* David Anthony et al., *5 Questions on Standing in the Wake of TransUnion*, TROUTMAN PEPPER (July 22, 2021), https://www.troutman.com/insights/5-questions-on-standing-in-the-wake-of-transunion.html [https://perma.cc/4QB9-PU7M].

[221] *TransUnion*, 141 S. Ct. at 2224 n.9 (Thomas, J., dissenting).

litigation could shift venues to state court where Article III standing is not a barrier to entry.[222] At the state court level, roughly half of states follow the Article III standing requirements introduced by *Lujan* and generally, state standing requirements are less stringent than their federal counterparts.[223] That said, if data breach cases were to be brought at the state level, there would be inequitable decisions of standing across jurisdictions depending on the standing requirements in each state, especially considering the wide variety of data security laws across different state lines.[224] Moreover, given the propensity for data breach cases to be brought as class actions, filing cases across multiple states could lead to further headaches and costs for plaintiffs if left without a rigid federal test for data breach standing.[225] Even more, although plaintiffs can pursue suits through state courts, they should not be foreclosed from federal courts just because of the highly restrictive Article III standing requirements that federal courts impose.[226]

B. Issues that May Arise with Standing Legislation or Unclear Tests of Standing

Kagan's *TransUnion* dissent put forth the solution that Congress should enact legislation to deal with issues of Article III standing directly, rather than having judges make these decisions.[227] However, given the ever-changing backdrop of data breaches and privacy, it would be inappropriate to implement legislation for determining standing in data breach cases.[228] As the *McMorris* decision acknowledges, "determining standing is an inherently fact-specific inquiry."[229] The legal landscape for data breaches is heterogenous and fluid, and the flexibility of common law should be preferred to the rigidity of congressional legislation when it comes to Article III standing.[230]

Moreover, congressional action would go directly against the very ideology that Article III standing law is built on:

---

[222] *Id.*; *see also* Anthony et al., *supra* note 220.

[223] Thomas B. Bennett, *The Paradox of Exclusive State-Court Jurisdiction over Federal Claims*, 105 MINN. L. REV. 1211, 1233 (2021); *see also* Anthony et al., *supra* note 220.

[224] Carson, *supra* note 87.

[225] Bennett, *supra* note 223; *see also* Anthony et al., *supra* note 220.

[226] Bennett, *supra* note 223; *see also* Anthony et al., *supra* note 220.

[227] *TransUnion*, 141 S. Ct. at 2226 (Kagan, J., dissenting).

[228] *See* Luca Anderlini et al., *State Law or Case Law?* 34 (London Sch. of Econ. & Pol. Sci Discussion Paper No. TE/2008/528, 2008), https://sticerd.lse.ac.uk/dps/te/te528.pdf [https://perma.cc/W2YT-MZ6].

[229] *McMorris*, 995 F.3d at 302.

[230] *See* Anderlini et al., *supra* note 228, at 34.

separation of powers.[231] Article III standing laws are in place "to prevent the judicial process from being used to usurp the powers of the political branches."[232] Allowing Congress to implement legislation on these issues would be to abandon standing requirements entirely, which could allow courts to exercise unchecked power to review issues more appropriately addressed in the legislative and executive branches.[233] Additionally, Justice Thomas's argument for private rights goes against *Spokeo's* established precedent that "Article III standing requires a concrete injury even in the context of a statutory violation."[234] Although modern standing law seems to have been made up in Scalia's 1992 *Lujan* decision, it acts independently to separate the branches of government and prevent overcrowding of the American court system.[235]

In addition to proposing congressional action, Justice Kagan joined Justice Thomas in proposing a common sense approach.[236] While the common sense approach offered by Justices Thomas and Kagan in their *TransUnion* dissents seems like a consumer-friendly alternative, it does not offer any real guidance.[237] Thomas and Kagan argued that standing in *TransUnion* should clearly be given merely by "tap[ping] into common sense," but there were five other Supreme Court Justices who thought otherwise.[238] Clearly, courts have different ideas of what common sense is, and if a test of common sense were applied in data breach cases, it could lead to vastly inconsistent decisions that differ on what amounts to standing.[239]

C. A Modified McMorris *Test*

While there are many proposed solutions to the Article III standing issue, the current *McMorris* test provides a rough draft that, if redesigned, would provide equitable relief to consumers.[240] The proposed modified *McMorris* test utilizes elements from the original *McMorris* test, but reworks the test

---

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

[232] *Id.*

[233] *See id.*

[234] Spokeo, Inc. v. Robins, 578 U.S. 330, 342 (2016).

[235] *See* Kennerly, *supra* note 119; *see also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 576–77 (1992).

[236] *See supra* Section II.D.

[237] *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2225–26 (2021) (Kagan, J., dissenting).

[238] *Id.* at 2226.

[239] *See id.* at 1115–26.

[240] *See* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 303 (2d Cir. 2021) (explaining the three factors of the test introduced in the decision).

into a two-step process. The first step of the modified test is a barrier to entry that considers whether cybercriminals have the ability to profit off stolen PII, while the second step consists of three factors—only one of which has to be met to grant plaintiffs standing—that consider the increased likelihood and intent of cybercriminals to profit off of stolen PII.

When looking at the current *McMorris* test, its third factor—the type of data exposed—is at the essence of any potential injury suffered from a data breach.[241] After all, the data that has been exposed determines the injury and extent of injury that may be felt by individuals.[242] Rather than being one of several factors to be weighed, the type of data exposed should be seen as a barrier to entry in the modified *McMorris* test. That is to say, the first step of the new *McMorris* test will be to determine if the type of data exposed leads to a high risk of identity theft, and if not, plaintiffs may not be granted standing. However, this barrier to entry should not be particularly difficult to meet for most data breach victims given the harm that can be done with a minimal amount of PII.[243] When determining what type of data is sensitive, such that there is an increased risk of future identity fraud, strict state notification statutes like those in California—which bear resemblance to the GDPR[244]—provide appropriate guidance in their definitions of "personal information."[245]

California describes sensitive PII that may lead to fraud or theft as:

> (1) [a]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
>
> (A) Social security number.
>
> (B) Driver's license number . . . .
>
> (C) Account number or credit or debit card number, in combination with any required security code, access code, or password . . . .
>
> (D) Medical information.

---

[241] *See In re* U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 58 (D.C. Cir. 2019).

[242] *See id*; *see also* Attias v. Carefirst, Inc., 865 F.3d 620, 627–28 (D.C. Cir. 2017).

[243] St. John, *supra* note 61; *see also What to Know About Identity Theft*, *supra* note 61.

[244] *See* Jonathan Keane, *From California to Brazil: Europe's Privacy Laws Have Created a Recipe for the World*, CNBC (Apr. 8, 2021, 1:32 AM), https://www.cnbc.com/2021/04/08/from-california-to-brazil-gdpr-has-created-recipe-for-the-world.html [https://perma.cc/P85M-84UH].

[245] *See* CAL. CIV. CODE § 1798.29 (West, Westlaw current with all laws through Ch. 997 of the 2022 Reg. Sess.).

> (E) Health insurance information.
>
> (F) Unique biometric data . . . .
>
> (G) Information or data collected through the use or operation of an automated license plate recognition system . . . .
>
> (H) Genetic data.[246]

Additional sensitive PII includes "[a] username or email address, in combination with a password or security question and answer that would permit access to an online account."[247] The modified *McMorris* test should use the California statute as a guideline for what constitutes sensitive PII that may lead to an increased threat of identity theft or fraud.

Once it has been determined that the PII is sensitive such that it may result in identity fraud or theft, the second step of the modified test will consider if any third party—especially a cybercriminal—has access and intent to profit off of that information, considering that there is an increased risk for identity theft any time a cybercriminal has access to PII.[248] That said, the other two factors introduced by *McMorris* consider whether there has been criminal use or intent to use the breached information.[249] If the first *McMorris* factor—whether there has been a targeted attack to obtain the data—is met, clearly the intent is to steal an identity or make fraudulent charges.[250] Additionally, if the second *McMorris* factor—whether at least some of the compromised data has been misused—is met, there is proof of the intent of hackers to use the breached data for identity theft or fraud.[251] When either of those two factors coincide with the data being sensitive PII, an increased risk of future harm is clear, and the plaintiff has standing.[252]

A final factor to consider is the length of time that the data has been available to outside parties. In 2021, the average company took 212 days to identify a data breach and an additional 75 days to contain it.[253] Still, companies like Marriot and Microsoft have recently experienced data breaches that

---

[246] *Id.*

[247] *Id.*

[248] *See In re* U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 58 (D.C. Cir. 2019).

[249] *See* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301–02 (2d Cir. 2021).

[250] *See id.* at 301.

[251] *See id* at 302; *see also In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d at 58.

[252] *See McMorris*, 995 F.3d at 301.

[253] IBM SEC., *supra* note 49, at 22.

divulged consumer information for several years at a time.[254] The longer it takes to detect a breach, the more time cybercriminals have to steal data, and in these prolonged breaches, victims may not feel the potentially severe consequences of identity theft for a number of years after the breach.[255] That said, when data is exposed for prolonged periods and victims are unaware of the breach, those victims "cannot protect themselves properly against a breach's implications," much less prove that they are at an increased risk of future harm.[256]

The longer the data is accessible to outside parties, the more time cybercriminals have to get their hands on it,[257] which makes the length of time that data has been available to outside parties an important factor to consider. Instances when there are prolonged uncontained data breaches demonstrate that the entity trusted with protecting the data was either negligent in their efforts to contain the breach or unprepared for the consequences of a breach to begin with.[258] Although it is difficult to quantify just how long sensitive PII needs to be available to an outside party in order for it to amount to an increased risk of future harm,[259] courts should consider this factor on a case-by-case basis. This final factor obviously allows for some interpretation by the court—which the updated test seeks to avoid—but it is necessary to account for the increased risk of harm to victims who have had their PII exposed for lengthy periods of time.[260] Thus, until the time needed to create an increased risk of future harm can be exactly quantified, courts should consider this factor on a case-by-case basis.

Ultimately, when looking at the updated *McMorris* test, standing should be given when the type of data is sensitive such that there is an increased risk of future identity theft or fraud, in addition to any one of the following factors: "(1) . . . the plaintiffs' data has been exposed as result of a targeted attempt to obtain the data; (2) whether any portion of the dataset has already been misused[;]" or (3) the data has been exposed for an excessive period

---

[254] *See* O'Donnell, *supra* note 44; *see also* Symanovich, *supra* note 4.

[255] *See* Shane Schick, *Data Breach Detection Time: How to Minimize Your Mean Time to Detect a Breach*, VERIZON, https://www.verizon.com/business/resources/articles/s/how-to-minimize-your-mean-time-to-detect-a-breach/ [https://perma.cc/N6A3-VA92]; *see also* FED. RSRV., *supra* note 66, at 17.

[256] *See* Thomas, *supra* note 86.

[257] *See* O'Donnell, *supra* note 44; *see also* IBM SEC., *supra* note 49, at 6.

[258] *See generally* Richardson et al., *supra* note 3 (explaining that many companies do not see it as a good investment to adequately prepare for data breaches).

[259] *See* IBM SEC., *supra* note 49, at 6.

[260] *See* O'Donnell, *supra* note 44.

of time as determined by the court on a case-by-case basis.[261] In the modified test, the first factor is a barrier to entry, and the other three factors are weighed equally, providing standing if any of them are met in combination with the first factor.

When considering if there exists an increased risk of future injury, the assessment ultimately comes down to whether cybercriminals have the ability and intent to profit off of stolen PII.[262] Accordingly, the DC Circuit decision of *In re U.S. Office of Personal Management Data Security Breach Litigation* granted standing based on the idea that when a hacker has both the intent and ability to use breached data for ill against data breach victims, there exists an increased risk of future injury for those individuals.[263] The reasoning used in *In re U.S. Office of Personal Management Data Security Breach Litigation* provides a jumping off point for the modified *McMorris* test. The sensitivity of the breached information offers a look into the ability of a third party to use breached data for ill, while the three factors in the second step of the modified *McMorris* test offer an indication of the third parties' intent in using that data.[264] Ultimately, when third parties possess the intent and ability to use breached data against individuals, there exists an increased risk of future harm. Accordingly, the modified *McMorris* test establishes an actual framework to determine the intent and ability of outside parties while also providing a firm guideline for plaintiffs to plead future injury.[265]

D. Legislation for Recovery of Reasonable Mitigation Expenses Taken

Although reworking the *McMorris* test may provide plaintiffs with an enhanced opportunity to be granted standing, it may also be inconsequential for some plaintiffs who take adequate precautionary steps to extinguish the risk of future identity theft.[266] *Clapper* and its progeny imply that victims of data breaches should sit back and hope for the best when their PII has been breached.[267] Doing otherwise would, in the eyes of

---

[261] *See* McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 303 (2d Cir. 2021) (explaining the three factors introduced in the decision).

[262] *See In re* U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 55–56 (D.C. Cir. 2019).

[263] *Id.*

[264] *See id.* at 58.

[265] *See id.* at 55–56.

[266] *See* Solove, *supra* note 31.

[267] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013).

the court, amount to "manufacture[d] standing."[268] By this logic, data breach victims are forced to choose between the lesser of two evils: (1) do nothing and potentially incur debilitating financial and mental harms if the PII ends up being used, or (2) spend valuable time and money to take preventive actions for a breach that was not their fault to begin with.[269]

Certainly, this seemingly unfair burden placed on the victims of data breaches stems from *Clapper's* ruling preventing recovery for "manufactured harms," and rulings like *McMorris* and *Tsao* that have followed in *Clapper's* footsteps.[270] However, the current data breach notification laws in place also contribute to the issue.[271] Relying on state notification laws that vary in language and stringency from state to state, consumers receiving these notifications may believe that they have an increased risk of fraud or identity theft even if they will ultimately not be granted standing in a potential suit.[272] In *Tsao*, for example, the plaintiffs were notified that their sensitive PII "may have been accessed" by outside third parties,[273] while in *McMorris* some victims of the breach were notified that their information had already been sent to third-parties.[274] Although neither of those cases granted the respective plaintiffs standing, the specific language of the notifications gave the individuals reason to believe that outside parties had access to their information and consequently, that taking preventive measures was in their best interests.[275] Unfortunately, there is currently a mess of lenient state data breach notification laws and a loophole that provides data breach defendants with a built-in defense when data breach victims actually do take reasonable preventative actions, leaving victims in an unwinnable situation.[276]

Given the plight of data breach victims, broad sweeping federal data breach notification laws are long overdue. California's data breach notification legislation is one of, if not the strictest notification law in place out of all fifty states.[277]

---

[268] *Id.*

[269] *See* Solove, *supra* note 31.

[270] *Clapper*, 568 U.S. at 402; McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301 (2d Cir. 2021).

[271] *See* Solove, *supra* note 31.

[272] *See* Lazzarotti & Gavejian, *supra* note 11.

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

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

[275] *See Tsao*, 986 F.3d at 1335; *see also McMorris*, 995 F.3d at 298.

[276] *See* Solove, *supra* note 31.

[277] *See* CAL. CIV. CODE § 1798.29 (West, Westlaw current with all laws through Ch. 997 of the 2022 Reg. Sess.); FOLEY & LARDNER LLP, *supra* note 107 (explaining the different definitions of "personal information" and "breach" as well as the risk of harm analyses and timing requirements in the data breach notification laws of all fifty states).

California data breach notification law requires a notification to "be written in plain language" and to present a minimum of listed required information under the headings "'What Happened,' 'What Information Was Involved,' 'What We Are Doing,' 'What You Can Do,' and 'For More Information.'"[278]

Federal data breach notification legislation should be modeled after California's current notification statute. To go one step further, federal notification legislation should allow for consumer recovery of reasonable expenses taken in efforts to mitigate the potential damages of a breach. Under the heading "What You Can Do,"—which describes what reasonable preventive actions individuals may take—victims of breaches should be granted the opportunity to recover for the expenses of those listed actions directly from the entity that exposed their information. This new legislation—an action taken separately from the new *McMorris* test—would provide recovery for all reasonable preventative measures taken subsequent to a breach, regardless of whether those victims taking defensive actions would ultimately be granted standing.

This solution would allow the plaintiffs in cases similar to *Whalen* and *Tsao* to at least recover for the expenses taken to mitigate the potential harms from a breach.[279] Under this new legislation, while plaintiffs who take preventative actions may still be denied standing to sue for increased risk of future injury, they would not be penalized for taking those preventive actions, as they effectively were in *McMorris*, *Tsao*, and *Whalen*.[280] Furthermore, this legislation could inspire companies to take data security measures more seriously. If companies were responsible for covering reasonable consumer expenditures following data breaches, executives may start to believe that extensive security measures are worth the cost.[281]

Even if the new *McMorris* test in a data breach case is met, a court would still have to analyze the facts of the particular case in court, and there is no telling if a plaintiff would be granted recovery. The financial and mental implications of having PII stolen and potentially used by cybercriminals are immense, yet under current standing law, taking preventative

---

[278] CIV. CODE § 1798.29(d)(1).

[279] *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017); *see also Tsao*, 986 F.3d at 1344.

[280] *See McMorris*, 995 F.3d at 298; *see also Whalen*, 689 F. App'x at 90–91; *Tsao*, 986 F.3d at 1344.

[281] *See* Richardson et al., *supra* note 3, at 229–30.

actions is viewed by courts as "manufactur[ing] standing."[282] Nationwide notification legislation that allows for recovery of reasonable expenditures taken to mitigate the potential harm will, at the very least, provide data breach victims with a way to recover expenses taken because of breaches that occurred through no fault of their own.

CONCLUSION

The volume of breached records has reached unprecedented highs in recent years, and that trend shows no signs of slowing down.[283] However, there is no existing federal data breach legislation, and decisions like *McMorris* and *TransUnion* make it increasingly difficult for victims of breaches to be granted Article III standing.[284] Pleading future injury in data breach cases is a problem that has only just begun to see the light of day and, considering the Court's decision in *TransUnion*, it is more important now than ever to implement a consumer-friendly approach to standing.[285] That said, being granted standing to sue only provides plaintiffs with a foot in the door to the legal process, merely allowing a lawsuit to be evaluated by a court of law.[286] Rearranging the *McMorris* factors and implementing federal data breach notification laws that allow for the recovery of reasonable expenses would provide American consumers with rightful remedies and keep the companies tasked with maintaining sensitive PII in check. When considering the immense damages that data breaches can wreak, substantive changes are past due to provide American consumers with protections and an equitable path to plead their cases in court.

John E. McLoughlin[†]

---

[282] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013); *see generally* IDENTITY THEFT RES. CTR., *supra* note 71, at 12 (explaining the mental tolls that data breaches impose on victims).

[283] Whitney, *supra* note 3.

[284] *See* Carson, *supra* note 87; *see also* Kornbacher et al., *supra* note 16.

[285] *See* Whitney, *supra* note 3.

[286] *See* Kennerly, *supra* note 119.

[†] J.D. Candidate, Brooklyn Law School, 2023; B.S.B.A., University of Miami, 2019. Thank you to the entire *Brooklyn Law Review* staff for their hard work throughout the publication process. Thank you to my friends, especially those at Brooklyn Law School, for their support and patience. Finally, thank you to my family, especially my parents, for their unwavering love, enthusiasm, and support.