ST. THOMAS JOURNAL OF COMPLEX LITIGATION

Volume 5 Spring 2019

STAND OR SIT? ARTICLE III STANDING IN CASES OF DATA BREACH: A UNIFORM SOLUTION

Maxwell Murray

STAND OR SIT? ARTICLE III STANDING IN CASES OF DATA BREACH: A UNIFORM SOLUTION

By: Maxwell Murray[1]

The world of technology has quickly and unexpectedly consumed our lives. Our dependence on technology, however, must be balanced with a significant tradeoff: accumulation of personal information. Today, most retail stores collect massive amounts of personal information such as names, birthdays, and social security numbers to store in their databases.[2] Security measures taken by these database holders may be inadequate to prevent data breaches by hackers and may only mitigate security risks, thus leaving consumers vulnerable.[3] These breaches often lead to fraudulent charges and misrepresentations known as identity theft or identity fraud.[4] Due to the large number of consumers affected, the high frequency of occurrences, and the prospect of costly litigation, class action suits are a crucial mechanism that allows consumers access to justice and monetary relief.[5] The question remains whether consumers who are victims of data breaches have Article III standing ("Standing") at the pleading stage such that they may bring a cause of action against these trusted holders of their personal information, absent the actual use of the stolen information by hackers. Have these consumers suffered an actual or imminent injury? Should there be an alternative test to determine standing in these circumstances, given the progressive nature of our society and its perprtual reliance on technology? Should there be uniform legislation to govern cybersecurity? If so, to what degree should consumers have Standing?

---

[1] Maxwell Murray, Juris Doctor Candidate May 2020, St. Thomas University School of Law, ST. THOMAS JOURNAL OF COMPLEX LITIGATION, *Member-Candidate*. I dedicate this article to my grandfather, Donald Murray ("Don"). Don went to law school at 38 while raising three kids and working a full-time job. He practiced law until he passed at the age of 90. My grandmother used to say, "There's not a crooked bone in his body," because of how honest and ethical he was. My grandfather's strength, perseverance, and curiosity for life is the reason I wrote this article in his name.

[2] In re Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018) (explaining some of the personal identifying information customers provide when shopping and the current litigation surrounding the standing document in data breach cases).

[3] *See* Corey Williams, *Current Cybersecurity Measures Not Enough to Stem the Tide of Breaches*, CENTRIFY (Nov. 5, 2015), https://blog.centrify.com/cyber-security-measures-not-enough-to-stem-the-tide-of-breaches/ (stating that despite companies' steps to prevent cybersecurity breaches, they must adopt more measures to help mitigate future occurrences, although they are still occurring).

[4] *See* Nicole Spector, *What is identity theft? Protection, how to report fraud, and more,* NBC NEWS (Mar. 26, 2018, 10:05 PM), https://www.nbcnews.com/storyline/smart-facts/identity-theft-facts-risks-what-consumers-can-do-n859011 (defining the term identity theft by the Department of Justice as occurring when anyone wrongfully obtains your personal data to be used toward a fraudulent end).

[5] *See* Catherine Piche, *The Cultural Analysis* of *Class Action Law*, 2 J. CIVIL L. STUD. 102, 127 (2009) (explaining the importance of class actions lawsuits); in *Western Canadian Shopping Centres v. Dutton*, the court stated:

> [B]y allowing fixed litigation costs to be divided over a large number of plaintiffs, class actions improve access to justice by making economical the prosecution of claims that would otherwise be too costly to prosecute individually. Without class actions, the doors of justice remain closed to some plaintiffs, however strong their legal claims. Sharing costs ensures that injuries are not left unremedied.

Western Canadian Shopping Centres v. Dutton, 2 S.C.R. 534, 28 (2001).

To have Standing, a plaintiff must first show that it has suffered an "injury in fact."[6] Upon the plaintiff's showing of an injury, the plaintiff must demonstrate that the injury is concrete and particularlized, and actual or imminent.[7] A plaintiff's injury may not be conjectural or hypothetical.[8] Second, the paintiff must show the injury is fairly traceable to the challenged action of the defendant.[9] Last, the plaintiff must proffer that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.[10]

Data breach issues concern the actual or imminent "injury in fact" requirement of Standing. The injury element has continuously developed over time and with data breach class actions presently taking center stage, the doctrine continues to evolve as courts face advancing modern technologies.[11] This has resulted in the current circuits' split on what plaintiffs must allege and whether plaintiffs who are victims of a data breach have Standing, absent the actual use of the stolen information by hackers.[12] The First, Second, Fourth, and Eighth Circuits have urged that the traditional "actual or imminent" test should be utilized to prove Standing.[13] While others, like the Third, Sixth, Seventh, Ninth, and D.C. Circuits, have adopted the "Substantial Risk" test, which asks whether there is a substantial risk that a harm will occur.[14] Because there is currently no uniform legislation requiring a certain level of cybersecurity or setting forth a timeframe for notification of a data breach, Congress should swiftly implement a uniform standard of security and an acceptable disclosure timeframe that all companies holding customers' personal information must adhere to.[15]

Accordingly, I propose a new test that acknowledges a heightened risk that the harm will occur ("Heightened Risk Test"), which should be implemented in all jurisdictions to determine Standing for the victims who find themselves in these predicaments. The test will be applied in cases where the defendants have (1) neglected to employ adequate security precautions and (2) failed to promptly notify customers of a data breach. The Heightened Risk Test will resolve the

[6] Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000) (laying out the foundation of the standing requirement provided in the case of Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).
[7] *Id.*
[8] *Id*.
[9] *Id.*
[10] *Id.*
[11] *See* Dominic Spinelli, *Data Breach Standing: Recent Decisions Show Growing Circuit Court Split,* AMERICAN BAR ASSOCIATION (Jan. 18, 2018), https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/data_breach_standing_recent_decisions_show_gowing_circuit_court_split/ (stating how there is a recent circuit split on offering different perspectives on what satisfies the injury requirement for Standing).
[12] *Id.*
[13] Petition for Writ of Certiorari at 13–15, In re Zappos.com, Inc., No. 18-225 (Jun. 29, 2018) (explaining how these circuits hold the injury requirement is not satisfied by merely pointing to the breach itself waiting for the possibility that data will be misused).
[14] *Id.* at 15–18 (finding that pleading the breach itself is enough to satisfy the injury requirement because it places the victims at a continuing, increased risk of fraud or identity theft).
[15] *See* Nuala O'Conner, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection (explaining how the U.S. is at the tipping point of a necessary implementation by Congress of a national cybersecurity and data breach notification standard); *How State Cybersecurity Regulations Drive Federal Action,* CORANET (Jul. 10, 2018), https://www.coranet.com/state-cybersecurity-regulations/ (describing how states approaches are providing the Federal government with models to consider in their effort to create its own nation-wide laws and how harmonization of State and Federal laws will reduce confusion and costs for companies doing business across state lines).

ambiguity inherent in the Standing question because it broadens the judicial standard in cases where a company has not followed the uniform standard and has, thus, unreasonably subjected consumers to a heightened risk of identity theft. The Heightened Risk Test would allow these victims to bring suit and acquire redress for their injuries.

Part I of this article explains the current issues with data breaches in the United States. Part II provides the arguments directly related to the concrete and actual or imminent element of Standing, by (a) discussing the arguments in favor of Standing and (b) discussing counterarguments to deny Standing. Part III provides the surrounding policy issues by (a) discussing the policy arguments in favor of Standing and (b) discussing the policy counterarguments to Standing. Part IV will briefly discuss the benefits of uniform legislation for data breaches and how it will benefit both, companies and consumers. Finally, Part V will conclude by offering an alternative test for courts to implement that will not only solve any ambiguities over Standing, but will also distinguish cases where defendants have failed to take proper measures to prevent and notify customers of a data breach.

I. The Current Issue with Data Breaches

The increasing number of consumers affected by data breaches every year is staggering.[16] Since 2005, there have been an estimated 11,239,084,942 records exposed from 8,891 data breaches.[17] In 2017, a study showed that the United States suffered approximately 1,579 recorded data breaches, which consisted of over 178 million records exposed to hackers.[18] When reconciled, these numbers indicate that a single data breach could impact the lives of millions of consumers in an instant.[19] According to a recent report, retail stores alone suffer an 80-90% fraudulent log in rate online by hacker's obtaining and using stolen data.[20] These breaches can also be very costly especially in the U.S. where the average cost of a single data breach is the highest at $7.91 million per breach.[21] The potential cost of a breach depends on several factors including, among other

[16] *See* Nate Lord, *The History of Data Breaches*, DIGITAL GUARDIAN (Apr. 6, 2018), https://digitalguardian.com/blog/history-data-breaches (indicating that the number of data breaches reported from 2013 to 2017 has more than doubled).

[17] *See Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches, (last visited Nov. 11, 2018) (showing a current, running tally of the number of data breaches and records exposed in the United States).

[18] *See* Identity Theft Resource Center, *Annual number of data breaches and exposed records in the United States from 2005 to 2018*, STATISTA, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited Oct. 2, 2018).

[19] *See* Mike Isaac and Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 million Users*, NEW YORK TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (stating Facebook exposed the records of fifty million users in a single breach); *see* Carole Theriault, *Top Five Data Breaches of Summer 2018*, TBG SECURITY (Sept. 13, 2018), https://tbgsecurity.com/top-five-data-breaches-of-summer-2018/ (stating Adidas exposed the records of "millions" of users and Timehop exposed the records of twenty-one million users in a single breach).

[20] *See* Dennis Green and Mary Hunbary, *If you shopped at these 16 stores in the last year, your data might have been stolen*, BUSINESS INSIDER (Aug. 22, 2018 5:49 PM), https://www.businessinsider.com/data-breaches-2018-4 (listing sixteen retailers who suffered a data breach, in 2017, and the facts that were involved for each instance, as well as, the effects to retailers as a whole).

[21] *See* Niall McCarthy, *The Average Cost Of A Data Breach In The U.S.*, FORBES (July 13, 2018 7:30 AM), https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-

things, the number of records stolen, the efficiency in identifying the incident, and the speed of the company's response.[22] On average, companies currently take 197 days to identify a data breach and an additional 69 days to contain it,[23] leaving consumers' information vulnerable for a period of almost nine months. Many state laws require a loose standard of thirty days to notify consumers of the breach, which essentially adds another month to the notification period.[24]

However, each state has implemented its own legislation mandating security standards and prompt notification policies, which companies must adhere to.[25] These standards vary widely from state to state making it difficult and confusing for companies to abide by them.[26] For example, a data breach in Maryland requires the state attorney general be notified; by contrast, New Jersey requires that the state police cybercrime unit be notified.[27] The Federal Trade Commission ("FTC") attempted to establish a data-security baseline.[28] However, due to the FTC's limited jurisdiction and companies' reluctance to comply with FTC regulations, the sixty different enforcement actions that were implemented have come to no avail.[29] Congress is currently working to draft a bill addressing the inconsistencies, but, unfortunately, there are many disagreements due to the legislation's proposed effect on all business, which makes the process to find a consensus extremely laborious.[30] Consequently, the increasing number of consumers affected by hackers, and the lack of suitable legislation to govern the issue, will only lead to more lawsuits. As a result of this ambiguity and its lack of uniformity, more cases concerning Standing will be heard.

II. Arguments Directly Related to the Standing Document

(a) An Actual or Imminent Injury Has Occurred

infographic/#20f99fca2f37 (describing the average financial impact data breaches have not only globally, but here in the U.S., and the different factors that contribute to this impact).

[22] *Id.* (providing that the potential costs of a breach fall in line with the number of records stolen and how the average cost per record applies).

[23] *Id.*

[24] *See* Charlie Mitchell, *Congress can't get over the hump on a law to notify consumers of hacks,* WASHINGTON EXAMINER (June 12, 2008 12:00 AM), https://www.washingtonexaminer.com/policy/technology/congress-cant-get-over-the-hump-on-a-law-to-notify-consumers-of-hacks (explaining the discrepancy in legislation throughout the United States and the importance of a uniform act by congress, including the current steps being taken, to regulate cybersecurity across the nation).

[25] *Id.* (providing examples of what different states' current regulations are and highlighting how different they are from each other).

[26] *Id.*

[27] *See* O'Conner, *supra* note 15 (providing examples of current legislation in certain states for notice requirements that could affect a company's disclosure procedures).

[28] *Id.* (describing the FTC's general power in this situation to prohibit "unfair and deceptive trade practices" under section 5 of the FTC Act).

[29] *Id.* (explaining how companies have begun to aggressively push back against the FTC's legal authority on data-security practices and its limited jurisdiction over certain entities such as; banks, insurance companies, nonprofit entities, and some internet service providers).

[30] *See* Mitchell, *supra* note 24.

Five circuits have argued that consumers have suffered an actual or imminent injury in cases where a consumer's information is stolen through a data breach but not actually used.[31] The Seventh Circuit has specifically stated on multiple occasions that consumers whose data is stolen have standing regardless if they allege any actual fraud or theft.[32] The argument rests on the notion that the stolen information itself is sufficient to satisfy the injury in fact requirement of Standing, and liability stems from what the company did or did not do before or after the breach to prevent it and notify affected individuals.[33]

In the case of *Barnes & Noble, Inc*., the Seventh Circuit reasoned as to why the consumer has satisfied this requirement:

> The plaintiffs have standing because the data theft may have led them to pay money for credit-monitoring services, because unauthorized withdrawal from their accounts cause a loss (the time value of money) even when banks later restore the principal, and because the value on one's own time needed to set things straight is a loss from an opportunity-cost perspective. These injuries can . . . support standing.[34]

That court further suggests, as do the First and Eleventh Circuits,[35] that the cancelling of credit cards, switching of card numbers for merchant automatic payments, costs of acquiring identity theft protection, aggravation in the process, etc., are some of the consequences consumers have to endure and act upon to protect themselves from any future loss.[36] These Courts also argue that data breach victims are at an increased risk of identity theft, large enough to satisfy the Substantial Risk Test.[37]

But what constitutes an increased risk that would satisfy this test? Substantial risk that a harm will occur, prompting plaintiffs to incur costs to mitigate or avoid harm, is satisfied as a result of the information obtained maliciously.[38] The hackers stole this information with the intent and

[31] *See In re Zappos.com, Inc.*, *supra* note 2 at 15–18. (stating the Third, Sixth, Seventh, Ninth, and D.C. Circuits have held the injury itself puts the victims at a substantial risk of harm occurring).

[32] *See* Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018) (explaining how consumers have standing because when their personal information is stolen they must take extra steps, costing time and money, in order to cure the situation and protect themselves).

[33] *See* Al Saikali, *The Target Data Breach Lawsuits: Why Every Company Should Care*, DATA SECURITY LAW JOURNAL (Dec. 30, 2013), https://www.datasecuritylawjournal.com/2013/12/30/the-target-data-breach-lawsuits-why-every-company-should-care/ (describing what complaints in the data breach legal landscape allege and how the time of filling may affect the merits of the case).

[34] *See Barnes & Noble, Inc.*, 887 F.3d at 828.

[35] *See* Saikali, *supra* note 33 (explaining the First and Eleventh Circuits' position on plaintiffs pursuing cognizable damages).

[36] *See Barnes & Noble, Inc.*, 887 F.3d at 827; Bill Hardekpof, *How to Protect Yourself After a Data Breach, FORBES (Nov. 16, 2017 2:50 PM), https://www.forbes.com/sites/billhardekopf/2017/11/16/how-to-protect-yourself-after-a-data-breach/#6402423546df* (listing seven things a consumer can do if they think their credit card information may have been stolen in a breach).

[37] *See In re Zappos, Inc.*, *supra* note 2, at 16.

[38] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) (discussing that Supreme Court cases do not uniformly require plaintiffs to show that it is literally certain that an injury will come about and that in some instances the Court has found standing based on a substantial risk that a harm will occur).

clear ability to use this data fraudulently[39] and their retention of this information subjects consumers to the ongoing threat of fraudulent use, even if it does not materialize for months or years.[40] During this time, many consumers are taking the measures stated above to protect their information in an effort to decrease their risk that any future fraud or identity theft will occur.[41] However, it may not be enough to ward off hackers from actually using the information, which still renders consumers at a substantial risk of harm.[42]

(b) An Actual or Imminent Injury Has Not Occurred

Alternatively, courts have argued there is no actual or imminent injury for Standing in cases where a data breach has occurred and consumers' information has not been used by the hackers.[43] Mere speculation that an injury may occur in the future is not enough to defeat the rigors of the "injury in fact" requirement of Standing, the injury must be certainly impending.[44] Allegations of a possible future injury do not satisfy the requirement for Standing[45] and many attorneys would argue that this prospect of future injury is a classic example of a "conjectural or hypothetical" injury.[46] This includes the chain of attenuation regarding the plaintiff's injury and whether the "if's" involved in the analysis would convince a court that the plaintiff is at an increased risk of harm substantial enough to qualify as an injury for Standing.[47] Common themes tend to emerge when analyzing these cases, which aids in explaining why courts often dismiss data breach class action lawsuits for lack of Standing.[48]

[39] *See* Attias v. Carefirst, Inc., 865 F.3d 620, 628–29 (D.C. Cir. 2017) (holding it is reasonable to infer that hackers have the intent and ability to use the stolen information and that this future risk of exposed information is not too speculative to establish standing).

[40] *See* Eva Velasquez, *Study Shows Link Between Breaches and Fraud*, CYBER SCOUT (June 10, 2014), https://cyberscout.com/education/blog/study-shows-link-between-breaches-and-fraud, (stating that victims of data breach are at the highest risk during the first twelve months after a breach occurs).

[41] *See Barnes & Noble, Inc.*,887 F.3d at 827.

[42] *See* Beth Givens, *Senate Judiciary And Banking Committee Hearing On Data Breaches, Panel One: Data Breach Law And Identity Theft Prevention*, PRIVACY RIGHTS CLEARINGHOUSE (May 21, 2014), https://www.privacyrights.org/blog/senate-judiciary-and-banking-committee-hearing-data-breaches-panel-one-data-breach-law-and (explaining how a study, done by Javelin Strategy and Research, showed that one in three data breach victims in 2013, also became a fraud victim in the same year).

[43] *See Stevens*, 884 F.3d at 844–901(stating the First, Second, Fourth, and Eight Circuits have concluded the mere possibility data will be misused in a manner that inflicts injury does not suffice).

[44] *See Clapper,* 568 U.S. at 409 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

[45] *See Whitmore*, 495 U.S. at 157 (explaining the petitioner's alleged injury is too speculative where petitioner would like to intervene as "next friend" for a fellow death row inmate, who waived appellate review, may eventually secure federal habeas corpus and that data could be used for comparative review in petitioner's case).

[46] *See Lujan*, 504 U.S. at 560 (finding that an injury must be "actual or imminent, not 'conjectural or hypothetical'").

[47] *See* Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 67-68 (2017) (explaining the various "if's" involved in the analysis of the injury requirement that include but are not limited to: if the plaintiff's personal information was compromised, if the information was obtained by an unauthorized outside party, and if the plaintiff's identity was actually stolen as a result of the breach).

[48] *See Clapper,* 568 U.S. at 414*;* Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) (holding that because the plaintiff began describing the injury with the word "if", the allegations were to attenuated to establish standing); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1052-53 (E.D. Mo. 2009) (finding the various if's and uncertainties that plaintiffs plead too attenuated and therefore not a strong enough argument to satisfy the Standing requirement).

Furthermore, hackers are beginning to delay their use of stolen information, and are subsequently able to build a richer profile on individuals that can be used for more lucrative exploits.[49] Generally, however, the time lapsed from when the breach occurred, to the time hackers use the stolen information for their financial gain typically occurs within a short period of time.[50] Lawsuits may take years before fully materializing, and as the time passes, the threat of injury becomes more and more speculative.[51] This leaves a gaping hole in the injury in fact requirement for Standing. This gap in time further strenghtens the defendant's argument that the harm is not fairly traceable to the defendant's data breach.[52]

There may be concern that relaxing the Standing requirement will risk future litigation over hypothetical questions, expanding the power of the courts to adjudicate issues that are not of case and controversy which is the essence of the Standing requirement.[53] There is a clear argument for both sides whether or not Standing should be allowed, bringing the judiciary to this current and difficult stalemate.

III. Surrounding Policy Issues

(a) Policy Argument For Allowing Standing

Companies holding consumer information are at the frontline of the battle against hackers attempting to infiltrate their customers' data. If these companies take affirmative steps to make it extremely difficult or nearly impossible for hackers to breach their data systems, hackers would be deterred from causing future harm to innocent individuals.[54] According to a study published in 2012, 97% of breaches are avoidable (in hindsight) through simple or intermediate controls.[55] Nevertheless, heightened security measures can also be costly to have and maintain, which is evidenced by companies preparing for the European Union's (the "EU") uniform data regulations

[49] *See* Beth Givens, *An On-The-Ground Look At Consumer Impacts Of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE (Jan. 12, 2016), https://www.privacyrights.org/blog/ground-look-consumer-impacts-data-breaches (explaining the effects of today's data breach environments to show the severity of the situation and what can be done moving forward to help prevent future breaches).

[50] *See 9 Minutes To Use Your Stolen Credentials?*, PRIVACY RIGHTS CLEARINGHOUSE (Jun. 8, 2017), https://www.privacyrights.org/blog/9-minutes-use-your-stolen-credentials (describing how the FTC created a fake customer database of approximately one hundred individuals and leaked it on a website where it only took hackers nine minutes before trying to fraudulently use the information).

[51] *See* Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (finding veterans whose information was on a stolen laptop was not enough for standing because they failed to show that the harm of future identity theft was certainly impending).

[52] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (quoting In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014)).

[53] *See Lujan*, 504 U.S. at 559–60.

[54] *See* Joe Panettieri, *Will New US Cybersecuirty Defense Strategy Deter Hackers, Cyberattacks?,* MSSP ALERT (Sep. 21, 2018), https://www.msspalert.com/cybersecurity-markets/americas/white-house-us-cybersecurity-strategy-policy/ (explaining new U.S. strategies in order to fight off hackers and that the U.S. has "suffered from a 'fundamental deterrence failure'" so far).

[55] *See* Verizon RISK Team, *2012 Data Breach Investigations Report*, DATA SEC. L.J. (2012) https://www.datasecuritylawjournal.com/files/2013/12/2012-Verizon-Data-Breach-Report.pdf (last visited Nov. 11, 2018) (showing a study on page three that describes how data breaches could have been avoided by without difficult or expensive countermeasures).

standard, also known as The General Data Protection Regulation ("GDPR"), implemented in May of 2018.[56]

Companies may not be motivated to implement these higher security measures if they do not have an extra incentive to protect the information they are holding, thereby leaving consumers to fend for themselves.[57] By allowing Standing and implementing a uniform standard of legislation, companies will be vulnerable to class action litigation that would inevitably result in harsh punishments dictated by the law. Companies would likely take action by incorporating measures, such as the hiring of a cyber security officer or committee.[58] These officials can aid companies in setting higher security restrictions or meeting a standard laid down through legislation by congress, knowing that costly litigation or settlement could be just around the corner.[59]

Further, permitting Standing may incentivize Congress to accelerate its efforts putting forth a bill addressing data breaches that may be signed into law. The constant threat of litigation would almost certainly expedite the passing of legislation, which is currently at a halt, due to numerous conflicting perspectives on the matter.[60] Unfortunately for these victims of data breaches, if Standing is not permitted, there will be no redress. This in turn will cause consumers to become discouraged from purchasing online or even in-store if they know they will not have judicial remedies for the loss of their personal information to the hands of criminals.[61] Consumers will be

[56] *See* Josh Fulinger, *Top cybersecurity facts, figures and statistics for 2018,* CSO ONLINE (Oct. 10, 2018 9:52 AM), https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html (explaining that of a survey of 300 tech executives at US, UK, and Japanese companies doing business in the EU, eighty-eight percent spent more than one million, and forty percent spent ten million or more, in preparation for the new EU regulations); *see* Michael Nadeau, *General Data Protection Regulation (GDPR): What you need to know to stay compliant,* CSO (Apr. 23, 2018), https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html (explaining that companies will now have just one standard to meet and that two-thirds of U.S. companies believe that the GDPR will force them to make a large investment because they will need to rethink their data security strategy and how to effectively administer it).

[57] *See* Rebecca Nanako Juchems, *Enough Is Enough: 2018 Has Seen 600 Too Many Data Breaches,* MEDIUM (Jul. 24, 2018), https://medium.com/@AxelUnlimited/enough-is-enough-2018-has-seen-600-too-many-data-breaches-9e3e5cd8ff78 (explaining how companies aren't protecting our information so we have to protect ourselves, and what steps we can take in order to do this).

[58] *See* Sharon Florentine, *Why you need a CSO/CISO*, CIO (Mar. 24, 2016), https://www.cio.com/article/3048074/careers-staffing/why-you-need-a-cso-ciso.html (stating that only about forty-nine percent of senior-level technology professionals during a few month period in 2015 stated the employed a CSO/CISO and the reasons why companies should have one).

[59] *See* Adam Janofsky, *Why Companies Should Prepare For More Data Breach Lawsuits*, THE WALL STREET JOURNAL (Dec. 11, 2017 5:12 PM), https://www.wsj.com/articles/why-companies-should-prepare-for-more-data-breach-lawsuits-1512563334 (explaining that in 2017 there have been several multimillion dollar settlements with companies that suffer data breaches including Target Corp. who agreed to pay $18.5 million).

[60] *See* Mitchell, *supra* note 24. (stating there are differences in opinions on what should be in the bill and the big issues are being narrowed but nothing will be finalized this year); *see* Derek Hawkins, *The Cybersecurity 202: The U.S. needs a law that requires companies to disclose data breaches quickly, cybersecurity experts say*, THE WASHINGTON POST (Oct. 15, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/10/15/the-cybersecurity-202-the-u-s-needs-a-law-that-requires-companies-to-disclose-data-breaches-quickly-cybersecurity-experts-say/5bc36a221b326b7c8a8d19a0/?utm_term=.93aa085eb805 (stating that there are competing bills on Capitol Hill and the issues involved have not been resolved).

[61] *See* Clare Meyer, *Measuring the Impact of Cyberattacks: Lost Revenue, Reputation & Customers*, SECURITY MAGAZINE (Feb. 2, 2017), https://www.securitymagazine.com/articles/87778-measuring-the-impact-of-

constructively forced to take precautions that a company should have otherwise taken at its own expense.[62] Consequently, consumers will be required to constantly replace credit cards, change passwords, pay for identity theft protection, and endure the stress and anxiety of the constant threat that their finances and personal life could be at stake at any moment.[63]

(b) Policy Argument Against Allowing Standing

Many advocates against allowing Standing would argue that allowing these victims of a data breach to bring class action lawsuits will force unnecessary litigation, even when some of these suits would not involve the actual fraudulent use of the information obtained through the breach.[64] Companies would be subject to pay out various sums of money in unnecessary settlements where, as some courts have argued, no injury has even taken place. It will be open season for attorneys to file suit, which would clog the judicial system.[65] With over 600 data breaches in 2018 alone,[66] there could be just as many suits to accompany them if Standing was allowed in every case. This would waste valuable time and resources, putting a strain on the judicial system. Because a breach is inevitable, and no system is flawless, it is very likely that innocent companies would have to pay heavy damages on top of the potential enormous costs to fix the breach.[67]

In addition to the consumer, companies are direct victims themselves.[68] Their reputations could be negatively affected by a breach, which would in turn surmount to a loss of business for the company.[69] The amount of time the systems are down causes loss of revenue, unexpected costs

cyberattacks-lost-revenue-reputation-customers (finding that twenty-nine percent of security professionals surveyed say their organization lost revenue and also cite losses of opportunity and customers after cyberattacks).

[62] *See* Consumer Reports Money Advisor, *How to protect yourself from Identity Theft*, CONSUMER REPORTS (Jul. 2010), https://www.consumerreports.org/cro/2010/07/protect-your-identity/index.htm (listing and describing eight ways to protect yourself from identity theft).

[63] *See Barnes & Noble, Inc*., 887 F.3d at 827.

[64] *See* John K. Higgins, *Data breach Lawsuits: A Growing Risk for E-Commerce*, TECHNEWSWORLD, (Oct. 6, 2018 5:00 AM), https://www.technewsworld.com/story/85607.html (stating federal courts of appeal have allowed consumers to pursue class action lawsuits even though the alleged injury from the breach was either small or even nonexistent).

[65] *See* Saikali, *supra* note 33 (describing that if anything less than a dismissal or summary judgment is entered in the case of Target, then expect the floodgates of data breach litigation to open).

[66] *See* Identity Theft Resource Center, *supra* note 18; Juchems, *supra* note 57 (describing recent data breaches and records exposed while highlighting some major breaches as well).

[67] *See* Adam Greenberg, *Plan ahead: Prepare for the inevitable data breach* (Sep. 2, 2014), https://www.scmagazine.com/home/security-news/features/plan-ahead-prepare-for-the-inevitable-data-breach/, SC MEDIA (explaining how companies should be prepared and focus on when, not if a data breach will occur because one will eventually happen, which could cost anywhere from thousands to millions of dollars).

[68] *See* Robert Abel, *Companies, customers will avoid you after a breach, survey says*, SC MEDIA (Nov. 9, 2018), https://www.scmagazine.com/home/security-news/companies-customers-will-avoid-you-after-a-breach-survey-says/ (finding that seventy-eight percent of individuals whose information was involved in a data breach said they would stop engaging with that brand while forty-nine percent said they would not use for an application or service that recently suffered a data breach).

[69] *See* Ponemon Institute LLC, *The Impact of Data Breaches On Reputation & Share Value*, CENTRIFY (May 2017), https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf (explaining how stock prices drop an average of five percent when the data breach is disclosed and how top executives agree the top impact of a data breach is loss of brand value and reputation); *see* Doug Drinkwater, *Does a data breach really effect your firm's*

to replace the compromised equipment, and other various expenses to remedy the situation and prevent further tarnishing of their name.[70] However, this could also deter companies from disclosing a breach all together.[71] These factors alone should be enough for companies to ensure their costumers' information is safe. Knowing all of the potential consequences of a breach and then revealing it to the public is a detriment in itself; but allowing suits to enter the courthouse doors in addition to these harms suffered by the company may create more issues then it resolves.

IV. Benefits of Uniform Legislation

First and foremost, uniform legislation will eliminate current conflicting state legislation, which will resolve the uncertainty within data breach reform.[72] With uniform legislation, companies can be held liable to allegations for failure to meet the uniform requirement. This would, in large part, resolve the issue of Standing because courts will have a solidified standard from which to render judgement. Similarly, the EU has enacted strict compliance rules to be followed, and are coined the granddaddy of all data regulations.[73] Although it may be costly to implement a uniform system of cybersecurity to prevent data breaches, the benefit would likely outweigh the cost simply because a breach itself can be a significant financial burden.[74] Although contingent on the size of the breach, a data breach against a company is likely to be much more expensive than the cost of maintaining adequate cybersecurity. [75]

reputation, CSO (Jan. 7, 2016), https://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html (stating that the reputational damage suffered by companies can translate directly into a loss of business but may not have much effect on the long term reputation).

[70] *See Dieffenbach*, 887 F.3d at 830; *see* Larry Ponemon, *Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT*, SECURITY INTELLIGENCE (Jul. 11, 2018), https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/ (describing two new factors used in the 2018 study of the average cost of a data breach and how the financial consequences of customers losing trust in your organization is another factor it be considered in analyzing a loss).

[71] *See* Eamon Javers, *Cyberattacks: Why Companies Keep Quiet*, CNBC, https://www.cnbc.com/id/100491610 (Updated Feb. 25, 2013 1:45 PM) (stating that companies may not want to reveal a breach due to concerns about the possibility of deterring potential or existing customers, damaging their stock value, or incurring potential legal liabilities).

[72] *See* O'Conner, *supra* note 15; Saikali, *supra* note 33 (explaining how state data breach laws are triggered by the location of the individual whose information is compromised, not by the location of the company that suffered the breach; meaning that every states' own requirements are in play in which each victim is located); Hawkins, *supra* note 60 (explaining that the United States plays by over 40 different cybersecurity rules that this is very costly, confusing, and a contradictory mess that only a national law can resolve).

[73] *See* Fulinger, *supra* note 56 (stating specifically that the EU's GDPR is the granddaddy of data regulation and providing that seventy-four percent of U.S. companies find that uniform legislation will be very effective); O'Conner, *supra* note 15 (stating the EU has become the focal point of the global dialogue on individual privacy and influencing other countries adopt the same framework); Mitchell, *supra* note 24 (stating the EU's data protection rule is far tougher than many state laws here in the U.S.).

[74] *See* Ponemon, *supra* note 70 (breaking down the average cost of a data breach per compromised record in 2018 and how all of these costs have increased year over year); *Id.* (stating the different factors involved in a data breach cost analysis and how simple measures can be taken to reduce the cost of a beach).

[75] *Id*. (providing statistical analysis to show that the average cost of a single breach in the U.S. is just under eight million dollars and that the larger the breach, the higher the cost). *See* McCarthy, *supra* note 21; Fulinger, *supra* note 56 (giving examples of what companies were spending in preparation for the GDPR where eighty-eight percent were spending over one million and forty percent spending over ten million).

Unfortunately, uniform legislation will partly shift the burden to consumers to protect their information; companies will be shielded by the law as long as they are complying with its parameters.[76] A new federal law requires credit bureaus to assist at-risk consumers by allowing them to place a freeze on their credit file upon contacting each of the three major credit reporting agencies, but more still needs to be done.[77] Consumers do not often take personal steps to protect their information, so the government should step in and provide assistance to combat the situation..[78]

Notwithstanding this reality, companies will still have to conform to strict measures and stay abreast of changing policies as data breach technologies and information are continually evolving.[79] However, it is not all bad for the consumer. A uniform standard will make it less likely that a breach would occur and could bring more awareness to this increasingly powerful yet adverse threat, not only by enactment of the law itself but by the notice requirements it could set in place.[80] Thus, consumers will be better equipped to help society prevent this invasion of privacy and, potentially, their finances.

Conclusion

Due to the surrounding policy issues and the fact that a breach can never be completely avoided, Congress should swiftly implement a strict uniform standard of cybersecurity for all companies that hold personal consumer information.[81] If a breach occurs, these companies must disclose the breach within a reasonable time period that would allow consumers to take prompt measures in further protecting their information. If companies adhere to this standard and the disclosure time frame, they will not be subject to suit when the consumers' stolen information, by way of a data breach, has not been fraudulently used. However, if companies fail to do so, the broad Heightened Risk Test will be implemented, subjecting them to costly class action suits where

[76] *See* Stacy Rapacon, *How to Protect Yourself From the Next Big Data Breach*, U.S. NEWS WORLD REPORT (Oct. 16, 2017 10:25 AM), https://money.usnews.com/money/personal-finance/banking-and-credit/articles/2017-10-16/how-to-protect-yourself-from-the-next-big-data-breachhttps://money.usnews.com/money/personal-finance/banking-and-credit/articles/2017-10-16/how-to-protect-yourself-from-the-next-big-data-breachhttps://money.usnews.com/money/personal-finance/banking-and-credit/articles/2017-10-16/how-to-protect-yourself-from-the-next-big-data-breach (stating that need to protect yourself is clear because data breaches have become certain to happen).

[77] *See* Lesley Fair, *New law, new consumer rights*, FEDERAL TRADE COMMISSION (Aug. 16, 2018 11:33 AM), https://www.ftc.gov/news-events/blogs/business-blog/2018/08/new-law-new-consumer-rights (describing how the Economic Growth, Regulatory Relief, and Consumer Protection Act allows consumers to freeze and unfreeze their credit file and the affects that has on businesses).

[78] *See* Christopher Mele, *Data Breaches Keep Happening. So Why Don't You Do Something?,* THE NEW YORK TIMES (Aug. 1, 2018), https://www.nytimes.com/2018/08/01/technology/data-breaches.html (describing recent high-profile data breaches that have occurred and how the majority of consumers are not taking proper steps to prevent further harm when one occurs); Verizon RISK Team, *supra* note 55 (showing a study on page three that explains consumers do not usually discover their own data breaches and third parties have to clue them in ninety-two percent of the time).

[79] *See* O'Conner, *supra* note 15.

[80] *See* Rahul Mukhi & Britta Redwood, *2018 Brings Continued Calls for a Federal Data Protection and Breach Statute*, CLEARLY CYBERWATCH (Jan. 10, 2018), https://www.clearycyberwatch.com/2018/01/2018-brings-continued-calls-federal-data-protection-breach-statute/ (stating new proposed legislation for uniform cybersecurity would require a thirty day disclosure period with some contingencies).

[81] *See* O'Conner, *supra* note 15.

standing will no longer be a matter of concern. Additionally, when a consumer's stolen information is actually and fraudulently used following a data breach, even when the company has abided by all formalities set by uniform legislation, those consumers will still be entitled to a cause of action against the company holding the data and seek relief for their damages, if any. This resolution provides clarity for all parties involved in the unpredictable realm of technology and its influence on the law.