INCENTIVIZING CYBERSECURITY COMPLIANCE IN THE NEW DIGITAL AGE: PREVALENCE OF SECURITY BREACHES SHOULD PROMPT ACTION BY CONGRESS AND THE SUPREME COURT♦

INTRODUCTION

In the new digital age, consumers are more inclined to trust companies with their personal and financial information as the amount of data stored and communicated electronically increases exponentially.[1] This trust is accompanied by the reasonable expectation that companies will implement cybersecurity policies sufficient enough to ensure the adequate protection of their information.[2] The increasing prevalence of data breaches, from the recent Dropbox invasion[3] to the Yahoo attack,[4] has led hackers to accumulate millions of consumers' personal and financial information at the expense of consumer privacy.[5] This raises important concerns about the ability of companies to implement self-policing security measures that protect consumer data.[6]

Victims of a data breach are at an increased risk of suffering financial harm and identity theft, despite not yet suffering actual harm.[7] Following a data breach, consumers rely on the judicial system to compensate them for the time and expenses incurred to mitigate the increased risk of future harm and return them to the position they would have been had the breach not occurred.[8] The serious financial and privacy implications of a data breach prompt questions about a victim's standing to sue companies that fail to protect their information

[1] *See* Thomas Martecchini, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After Clapper v. Amnesty International USA*, 114 MICH. L. REV. 1471, 1472 (2016).
[2] *Id.*
[3] *See* David Meyer, *How to Check if You Were Caught up in the Dropbox Breach*, FORTUNE (Aug. 31, 2016, 4:48 AM), http://fortune.com/2016/0/31/dropbox-breach-passwords/.
[4] *See* Madhumita Murgia, *Yahoo Hacking—what you need to know*, FIN. TIMES (Sept. 23, 2016), https://www.ft.com/content/266aa154-8165-11e6-8e50-8ec15fb462f4.
[5] *See* Resnick v. AvMed, Inc., 693 F.3d 1317, 1329 (11th Cir. Fla. 2012); Rachael King, *Data Breaches Rise While Companies Struggle With Detection*, WALL ST. J. (May 5, 2016, 6:41 PM), http://blogs.wsj.com/cio/2016/05/05/data-breaches-rise-while-companies-struggle-to-detect-them/.
[6] *Id.*
[7] *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014).
[8] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

following a breach.[9] Although companies are often also the victims of hacker infiltration, it is argued that they should be responsible for the confidentiality of their consumers' information.[10] Consequently, they should be liable for the increased risk that their consumers' confidential information will be exposed resulting from their failure to implement necessary security measures.[11]

When *Clapper v. Amnesty International* was decided in 2013, the Supreme Court deviated from its well-established "objectively reasonable likelihood" standard, to require that the plaintiff's injury be "certainly impending."[12] This heightened standard made it considerably more difficult for victims of a data breach to hold companies accountable for insufficient security measures,[13] dissuading victims from engaging in litigation. As a result, the rigorous standard fails to incentivize corporations to protect consumer data in fear of litigation and, thus, significantly contributes to the increasing prevalence of data breaches. Nonetheless, *Clapper* contains a footnote indicating that the Court will not always use the "certainly impending" standard.[14] It specifies that the Court "[does] not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will [occur,] . . . [and] have found standing based on a 'substantial risk' that the harm will occur."[15]

This issue is exacerbated by the fact that not all circuits apply the "certainly impending" standard to facts that depart from *Clapper's* unique national security context. As a result, a circuit court split concerning the scope of *Clapper* has developed.[16] The injury-in-fact standing requirement is the main source of controversy surrounding the split.[17] The inconsistent circuit court rulings, whereby certain circuits confer standing to sue for an increased risk of future harm while others do not, fail to provide the necessary guidance, incentives, and predictability for companies to structure their businesses to avoid data

[9] *See* Bill Sampson et al., *A Standing in Data Breach Cases: Changing Legal Landscape and a Few Suggestions for Counsel*, IN-HOUSE DEF. Q. (2016), file:///Users/cristiana/Downloads/IDQ201601SampsonSaikaliSchwaller.pdf.
[10] *See* David M. Ewalt, *Are Companies Liable For ID Data Theft?*, FORBES (Apr 14, 2005, 3:00 PM), https://www.forbes.com/2005/04/14/cx_de_0414liability.html#2c88702e5be4.
[11] *Id.*
[12] Clapper v. Amnesty Int'l U.S.A, 133 S. Ct. 1138, 1141 (2013).
[13] *See In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 956 (D. Nev. 2015).
[14] *Clapper*, 133 S. Ct. at 1150.
[15] *Id.*
[16] Martecchini, *supra* note 1.
[17] *See* Miles L. Galbraith, *America the Virtual: Security, Privacy, and Interoperability in an Interconnected World: Comment: Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U.L. REV. 1365, 1386–87 (2013).

breaches.[18]

This Note proposes a comprehensive scheme, whereby the legislature and judiciary collaborate to minimize security breaches. The scheme is intended to incentivize companies to sufficiently protect consumer data, while also considering that companies are often the victims of data breaches. It will first argue that, despite the aforementioned *Clapper* footnote, the Supreme Court should more definitively resolve the circuit court split by confining *Clapper's* "certainly impending" standard to the national security context in which it arose. This would significantly increase the chance for plaintiffs to sue for an increased risk of future injury.[19] Next, it will argue that Congress should adopt a federal statute requiring the implementation of cybersecurity policies and internal control as an integral part of companies' compliance programs. The extent of the policies would vary according to the company's net worth. Finally, it will argue that when plaintiffs sue for an increased risk of future harm alleging that a company negligently failed to implement reasonable security measures, the judiciary should evaluate the company's compliance with the statute. If the court determines that the company has made a reasonable good faith effort to comply, the court should mitigate its damages accordingly.

I. PURPOSE AND DEVELOPMENT OF THE STANDING DOCTRINE

The purpose of the standing doctrine is to preserve the judiciary's role in only hearing cases or controversies as defined by Article III § 2 of the Constitution.[20] The "case or controversy" requirement is fundamental to a democracy designed to protect the separation of powers between the federal government and the judiciary.[21] It has been held that "[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies."[22] Although it is a federal requirement often adopted by state courts, "requirements [limiting] federal judicial authority do not bind state courts,"[23] and it is argued that imposing federal requirements would "unnecessarily intrude on the states as distinct sovereignties."[24] Failure to fulfill the "case or

[18] Alison Frankel, *New Cert Petition: SCOTUS Must Decide When Data Breach Victims Can Sue*, REUTERS (Oct 31, 2017, 2:20 PM), https://www.reuters.com/article/us-otc-databreach/new-cert-petition-scotus-must-decide-when-data-breach-victims-can-sue-idUSKBN1D02M2.
[19] Martecchini, *supra* note 1; Galbraith, *supra* note 17.
[20] *See* Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 125 (1998).
[21] *See* Allen v. Wright, 468 U.S. 737, 750 (1984).
[22] Daimler Chrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006).
[23] Brian A. Stern, *An Argument Against Imposing the Federal "Case or Controversy" Requirement on State Courts*, 69 N.Y.U. L. REV. 77, 77 (1994).
[24] *Id.* at 78.

controversy" requirement, leading to a lack of standing to sue, is a defect in subject-matter jurisdiction that "may properly be challenged under Rule 12(b)(1)."[25] The constitutional standing requirements cannot be applied mechanically, as their application is heavily dependent on the facts and circumstances surrounding a particular case.[26] Although the "standing doctrine incorporates concepts concededly not susceptible of precise definition,"[27] case law in the data breach context has developed the standing doctrine and guides courts by more precisely defining the standing requirements.[28] Additionally, while the standing doctrine limits a court's jurisdiction, the separation of powers permits "the gradual clarification of the law through judicial application."[29]

II. STANDING REQUIREMENTS

A. *Burden of Proof*

The three constitutional elements necessary to establish standing are injury-in-fact, causation and redressability.[30] The requirements are designed to ensure that the litigants with the most stake in the outcome of the litigation are the ones advocating their suit,[31] to prevent a floodgate of litigation[32] and to decide cases based on concrete and particularized facts applicable to real cases and controversies.[33] To prove each element, "[t]he party asserting federal jurisdiction bears the burden of establishing these requirements at every stage of the litigation."[34] Thus, plaintiffs must prove that a favorable decision is likely to provide the relief they request and redress the personal injury they suffer from as a result of defendant's unlawful conduct.[35]

B. *Causation and Redressability Requirements*

This Note will not focus heavily on the causation and redressability requirements, as the primary inconsistency among circuits in the data breach context involves the injury-in-fact requirement. To satisfy the causation requirement, the plaintiff must prove a fairly

[25] Wright v. Incline Vill. Gen. Imp. Dist., 597 F. Supp. 2d 1191, 1199 (D. Nev. 2009); *see Allen*, 468 U.S. at 750; Liberte Capital Grp., LLC v. Capwill, 248 F. App'x. 650, 672 (6th Cir. 2007); *see* Sampson, *supra* note 9.
[26] *Liberte*, 248 F. App'x at 672; Lujan v. Def. of Wildlife, 504 U.S. 555, 562 (1992).
[27] Allen v. Wright, 468 U.S. 737, 751 (1984).
[28] *Id.*
[29] *Id.* at 752.
[30] *See* Delta Air Lines, Inc. v. Export-Import Bank, 85 F. Supp. 3d 250, 260 (D.D.C. 2015).
[31] *See Allen*, 468 U.S. at 752.
[32] *See* Toby J. Stern, *Federal Judges and Fearing the "Floodgates of Litigation"*, 6 U. PA. J. CONST. L. 377, 384 (2003).
[33] *See* Lujan v. Def. of Wildlife, 504 U.S. 555, 560 (1992).
[34] Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010).
[35] *Id.*; *see also* Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 96 (1998).

traceable casual connection between the injury suffered by the plaintiff and the defendant's conduct that the plaintiff is complaining of.[36] To satisfy the redressability requirement, the plaintiff must prove that it is likely, not merely speculative, that the injury complained of will be redressed by a favorable decision.[37] This analysis will consider whether actions by intervening parties not before the court will make it difficult for the remedy issued by the court to adequately resolve the injury.[38]

C. *Injury-in-Fact Requirement*

The injury-in-fact requirement is the subject of dispute among circuit courts. An injury-in-fact is the "invasion of a legally protected interest."[39] To satisfy the injury-in-fact requirement, the injury must be concrete and particularized, as well as real and imminent.[40] A concrete and particularized injury means that the plaintiff is the party who in fact suffered the injury and is thus the appropriate party to sue.[41] The relevant determination is whether the plaintiff, or class of plaintiffs, has a substantial enough stake in the outcome of the litigation for the court to decide the case on its merits.[42] Moreover, the injury "must be concrete in both a qualitative and temporal sense" as well as "distinct and palpable, as opposed to merely [a]bstract."[43] A real and imminent injury means that it is not merely speculative or conjectural, but rather reasonably or highly probable to occur.[44] However, *Clapper's* heightened standing requirement necessitates that the injury be "certainly impending."[45] Nonetheless, many courts limit the "certainly impending" standard to cases brought under 50 U.S.C. § 1881(a), cases dealing with the Federal Intelligence Surveillance Act and national security more broadly.[46]

D. *Prudential Limitations of Standing*

Unlike the constitutional requirements, prudential limitations of standing can be waived by Congress to confer standing.[47] These

[36] *See Lujan*, 504 U.S. at 562.
[37] *Id.* at 561.
[38] Michael S. Moore, *Causation and Responsibility: An Essay in Law, Morals, and Metaphysics*, 14 New Crim. L. Rev. 162, X (2009).
[39] *Lujan*, 504 U.S. at 560.
[40] *Id.*
[41] *Id.* at 581.
[42] *See* U.S. CONST. art. III, § 2; L.A. v. Lyons, 461 U.S. 95, 101 (1983).
[43] Whitmore v. Arkansas, 495 U.S. 149, 155 (1990).
[44] *Id.*
[45] Clapper v. Amnesty Int'l U.S.A, 133 S. Ct. 1138, 1141 (2013).
[46] *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014).; *see also In re* Sony Gaming Networks, 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014); Moyer v. Michaels Stores, Inc., 2014 WL 3511500, at *5 (N.D. Ill. 2014).
[47] *See* Brian A. Stern, *An Argument Against Imposing the Federal "Case or Controversy" Requirement on State Courts*, 69 N.Y.U. L. REV. 77, 83–84 (1994).

limitations are only analyzed after the plaintiff satisfies the constitutional standing requirements.[48] A prudential limitation that is relevant to the data breach context is that courts are reluctant to grant standing to third party plaintiffs asserting others' rights.[49] Plaintiffs will more likely establish standing by alleging an increased risk of future harm if they challenge the company's conduct as applied to the particular plaintiff, as opposed to suing on behalf of others.[50] Similarly, plaintiffs are typically unable to sue for generalized grievances, including widely shared harms.[51] Generalized grievances are "more appropriately addressed in the representative branches,"[52] such as through legislation that will be broader in scope than a lawsuit. However, unlike widely shared harms, particularized harms fall within the injury-in-fact requirement and thus cannot be waived by Congress.[53]

E. *Case Law Exemplifying Injury-in-Fact Requirement*

An infamous case exemplifying the injury-in-fact requirement involves a citizen suit provision, which allows broad citizen oversight to enforce statutes by creating federal standing to sue.[54] In one case, the Endangered Species Act (ESA) had a citizen suit provision conferring standing on citizens alleging that departments bound by the ESA violated their duties to consult with other agencies to protect endangered species.[55] The Court held that the plaintiffs, members of Defenders of Wildlife, did not have standing to sue merely because the departments' failure to fulfill their duties interfered with their ability to see endangered species during their future travels.[56] The plaintiffs did not suffer a concrete and particularized harm because they did not have a personal stake in the outcome of the litigation.[57] The plaintiffs were required to demonstrate that they would be injured by the lack of department oversight because they were using the habitats containing the wildlife. Moreover, the Court held that their injury failed to meet the real and imminent requirement, since their travel plans were only tentative, thus their injury was not highly likely to occur.[58] The Court

[48] *Id.*
[49] *Id.*
[50] *See* Bradford C. Mank, *Prudential Standing Doctrine Abolished or Waiting for a Comeback?: Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 18 U. PA. J. CONST. L. 213, 217 (2015).
[51] *See* Allen v. Wright, 468 U.S. 737, 751 (1984).
[52] *Id.*
[53] Stern, *supra* note 23, at 83–84.
[54] Lujan v. Def. of Wildlife, 504 U.S. 555, 572 (1992).
[55] *Id.* at 558–59.
[56] *Id.* at 556.
[57] *Id.* at 565–66 ("To say that the Act protects ecosystems is not to say that the Act creates (if it were possible) rights of action in persons who have not been injured in fact, that is, persons who use portions of an ecosystem not perceptibly affected by the unlawful action in question.").
[58] *Id.* at 564.

held that the plaintiffs could successfully establish standing if they could demonstrate a more definitive plan to see the endangered wildlife.[59] In addressing the prudential limitations on standing, the Court held that the plaintiffs were merely two out of billions of individuals that were part of a globally connected eco-system and thus their injuries were "generalized," as the government's failure to abide by the law is both widely shared and not particularized.[60]

III. CLAPPER V. AMNESTY INTERNATIONAL

In *Clapper v. Amnesty International*, plaintiffs, all of whom worked in professions requiring them to gather information from foreigners abroad, alleged that the government was intercepting their communications with their clients.[61] The plaintiffs argued that the Foreign Intelligence Surveillance Act was likely intended to target foreign individuals such as their clients.[62] They argued that, as a result, the government's interception of their communications prevented them from adequately protecting their clients.[63] An amendment to the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881(a), eliminated certain government requirements to obtain permission from the Court to intercept certain communications, giving the government significant ability to accomplish its intended surveillance.[64] The plaintiffs alleged future injury, claiming there was an objectively reasonable likelihood their communications would be intercepted under § 1881(a),[65] and also present injury, claiming that § 1881(a) had already required plaintiffs to assume expensive measures to protect the confidentiality of their communications.[66]

Writing for the majority, Justice Alito held that plaintiffs' allegations of future injury failed to meet the imminence requirement of injury-in-fact because their claims merely speculated about future injury.[67] Consequently, he required that their injury be certainly impending,[68] a higher standard than the reasonably or highly probable standard required of prior rulings.[69] Moreover, Justice Alito held that their allegations of present injury relied on a "highly attenuated chain of

[59] *Id.*
[60] *Id.* at 573–75.
[61] Clapper v. Amnesty Int'l U.S.A, 133 S. Ct. 1138, 1156–57 (2013).
[62] *Id.* at 1148.
[63] *Id.*
[64] *Id.* at 1144.
[65] *Id.* at 1143.
[66] *Id.* at 1146.
[67] *Id.* at 1143.
[68] *Id.* at 1147.
[69] *Id.* ("As an initial matter, the Second Circuit's 'objectively reasonable likelihood' standard is inconsistent with our requirement that 'threatened injury must be certainly impending to constitute injury in fact.'").

possibilities,"[70] and that plaintiffs "[could not] manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[71] The Court held that mitigation expenses did not constitute actual injury without demonstrating the existence of an imminent harm.[72]

Justice Alito also held that the plaintiffs could not certainly or affirmatively demonstrate that the government would target their communications, but rather could only hypothesize how the government would use its discretion.[73] He held that even if they proved the government requested the communications, the plaintiffs could only speculate whether the Court would authorize the government's request.[74] Furthermore, if the Court did approve, the plaintiffs were also speculating that the government would be successful in acquiring the communications.[75] The Court said in, dictum, that attorneys of clients who knew their communications were being intercepted, and those prosecuted with information used in §1881(a), would have standing.[76] This case transformed the standing requirements and created a heightened bar for plaintiffs.[77]

A. *Clapper Dissent*

Clapper's pragmatic dissent rejects Justice Alito's heightened standing requirement. Justice Breyer, joined by Justices Ginsburg, Sotomayor, and Kagan, claimed that from a practical standpoint, supported by inferences from the record involving the Department of National Security's operations in practice, it was highly likely that the government would intercept plaintiffs' communications.[78] He contended that the plaintiffs were engaged in the very communications that the government was seeking to intercept under the Act and the government was strongly motivated to receive such communications.[79] Accordingly, the plaintiffs' allegations were not based on unreasonable fear and speculation, but on facts proving that interception was highly likely.[80] They reasoned that the government's past behavior demonstrated an

[70] *Id.* at 1148.
[71] *Id.* at 1151.
[72] *Id.* at 1152.
[73] *Id.* at 1149.
[74] *Id.* at 1150–51.
[75] *Id.* at 1149–50.
[76] *Id.* at 1153.
[77] *Id.* at 1160. ("[A]s the majority appears to concede, *certainty* is not, and never has been, the touchstone of standing. The future is inherently uncertain. Yet federal courts frequently entertain actions for injunctions and for declaratory relief aimed at preventing future activities that are reasonably likely or highly likely, but not absolutely certain, to take place. And that degree of certainty is all that is needed to support standing here.").
[78] *Id.* at 1157–58.
[79] *Id.* at 1158.
[80] *Id.* at 1155.

interest in seeking information about detainees through surveillance of electronic information,[81] the government had the capacity and a strong motive to intercept these communications,[82] and the intelligence court rarely declined authorization of a government's request.[83] Consequently, the dissent concluded that because the government was interfering with plaintiffs' professional duties, it was rational to bring a lawsuit and take precautions to avoid interception.[84]

IV. COURT CONSENSUS ON STANDING TO SUE FOR FINANCIAL HARM OR IDENTITY THEFT

Most courts concede that alleging financial harm is sufficient to satisfy the injury-in-fact component of standing.[85] The injury is concrete and particularized if the party suing is the one who incurred the financial harm[86] and it is also real and imminent if the injury had already occurred and a monetary value could be ascertained to proportionately represent the plaintiff's harm.[87] Moreover, financial harm satisfies the causation requirement because the plaintiff likely incurred financial loss as a result of the company's negligent security measures.[88] It also satisfies the redressability requirement because a favorable decision will often result in the company reimbursing the plaintiff.[89] One court even held that plaintiffs satisfied the injury-in-fact requirement when they were already reimbursed for their financial loss.[90]

Plaintiffs can also usually establish standing by alleging identity theft, despite no actual financial harm.[91] In one case, tapes containing millions of medical records were stolen.[92] One of the plaintiffs alleged that loans were taken out using his personal information and others claimed to receive unsolicited phone calls disclosing their personal information.[93] The company who owned the files offered the parties free

[81] *Id.* at 1158.
[82] *Id.*
[83] *Id.* at 1159.
[84] *Id.* at 1158–60.
[85] *See* Robert D. Fram et al., *Standing in Data Breach Cases: A Review of Recent Trends*, COVINGTON & BURLINGTON LLP (Nov. 9, 2015), http://www.bna.com/standing-data-breach-n57982063308/.
[86] *See also* In re Target Corp., 66 F.Supp. 3d 1154, 1159 (D. Minn. 2014); *In re* Hannaford Brothers Co., 293 F.R.D. 21, 35 (D. Me. 2013).
[87] *See also In re* Ill. Bell Tel., 994 N.E.2d 553, 558 (Ill. App. Ct. 2013).
[88] Tierney v. Advocate Health and Hosps. Corp., 2014 WL 5783333, at *2 (N.D. Ill. 2014).
[89] *Id.*
[90] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696–97 (7th Cir. 2015).
[91] *See* Resnick v. AvMed, Inc., 693 F. 3d 1317, 1330 (11th Cir. 2012); *see also In re* Sci. Applications Int'l Corp., 45 F. Supp. 3d 14, 19; *see generally* Corona v. Sony Pictures Entm't, Inc., No. 14-CV-09600 RGK, 2015 U.S. Dist. LEXIS 85865, at *6 (C.D. Cal. June 15, 2015).
[92] *See In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 20 (D.D.C. 2014).
[93] *Id.* at 21.

credit monitoring and identity-theft protection for one year.[94] The court held that plaintiffs alleging their information, including their identity, was actually accessed and misused may establish injury-in-fact sufficient to confer standing.[95] Nonetheless, the court imposed the prudential limitation that the few plaintiffs that could both allege and prove their injuries out of millions of alleged victims could not extend their claims to confer standing on the other victims.[96]

V. COURT SPLIT ON STANDING TO SUE FOR INCREASED RISK OF FINANCIAL HARM OR IDENTITY THEFT

As opposed to allegations of actual financial harm or identify theft that typically give rise to standing without dispute, whether allegations of an increased risk of future harm warrant standing to sue is controversial among circuits.[97] The split derives from plaintiffs suing before their data is used inappropriately.[98] The majority of courts, notably the First and Third Circuits,[99] hold that the mere existence of a data breach is insufficient to establish standing because "the risk of plaintiffs' stolen data being misused in the future [as a result of the breach], and therefore the risk of plaintiffs suffering an injury, is not imminent."[100] On the other hand, the minority of courts, notably the Seventh and Ninth Circuits,[101] confer standing for an increased risk of future harm resulting from a breach.[102] These courts hold that plaintiffs may establish an imminent and non-speculative harm by reasoning that hackers steal consumer information intending to fraudulently or inappropriately use the identifying data in the future.[103] Since many consumers take various steps to protect their data following a breach,

[94] *Id.* at 20.
[95] *Id.* at 31; *see generally Corona*, 2015 U.S. Dist. LEXIS 85865.
[96] *In re SAIC*, 45 F. Supp. 3d at 34; *see generally* Green v. eBay No. 14-1688, 2015 U.S. Dist. LEXIS 58047 (E.D. La. May 4, 2014).
[97] Fram, *supra* note 85.
[98] *See* Wright v. Incline Vill. Gen. Imp. Dist., 597 F. Supp. 2d 1191, 1199 (D. Nev. 2009); *see* Sampson, *supra* note 9.
[99] Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011); Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011) (holding that the plaintiffs did not have standing to sue because their harm was not imminent but was rather based on the fear of hypothetical harm by a third party).
[100] Brittany Robbins, *Who Can Sue after a Data Breach?*, A.B.A. (Mar. 14, 2016), http://apps.americanbar.org/litigation/committbusinesstorts/articles/winter2016-0316-who-can-sue-after-a-data-breach.html. ("[I]t is well settled that a claim of injury generally is too conjectural or hypothetical to confer standing when the injury's existence depends on the decisions of third parties . . . Plaintiffs cannot 'prophylactically spen[d] money' to ease their fear of future harm and rely on that cost to establish standing.").
[101] *See* Pisciotta v. Old Nat. Bancorp, 499 F.3d 629 (7th Cir. 2007); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).
[102] *See Expert Q&A: Standing in Data Breach Class Actions*, PRAC. L. INTELL. PROP. & TECH., http://www.kslaw.com/imageserver/KSPublic/library/inthepress/4-3-15_PracticalLaw.pdf.
[103] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

courts hold that the costs incurred to mitigate this future injury constitutes an injury-in-fact that satisfies Article III standing.[104] These courts hold that the cost of mitigating harm creates "a certainly impending future harm from the theft of [plaintiffs'] personal data."[105]

The circuit court split, which can be explained both by jurisdictional precedent and factual distinction, has created unpredictable and inconsistent results concerning the requirements necessary to prove standing.[106] To further exemplify the split, it is important to understand both sides: circuits that confer standing for harm caused by an increased risk of future injury[107] and circuits that deny standing on this basis.[108] The cases where plaintiffs allege an increased risk of future financial harm and identity theft are the most common due to the increasing prevalence of data breaches in recent years.[109]

VI. COMPETING INTERPRETATIONS OF CLAPPER: CASES CONFERRING STANDING FOR INCREASED RISK OF FUTURE INJURY

A. *Real and Imminent Threat of Future Injury*

In re Adobe and *Neiman Marcus* are two prominent cases where the court established standing for allegations of future injury.[110] In *In re Adobe*, the court held that the plaintiffs' risk was real and imminent when their financial information was posted online after Adobe's system was hacked and consumers' credit card information was decrypted.[111] The plaintiffs alleged future harm due to the financial burden of purchasing services to mitigate the risk.[112] The court held that the mitigation costs represented another injury-in-fact in addition to the increased risk of future harm and was sufficient to confer standing.[113]

---

[104] *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1217 (N.D. Cal. 2014).
[105] *Id.*
[106] Martecchini, *supra* note 1.
[107] *See* Pisciotta v. Old Nat. Bancorp, 499 F.3d 629 (7th Cir. 2007); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010); *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197 (N.D. Cal. 2014); Denney v. Deutsche Bank AG, 443 F.3d 253 (2d Cir. 2006); *In re* Sony Gaming Networks, 996 F. Supp. 2d 942 (S.D. Cal. 2014).
[108] Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007); Moyer v. Michaels Stores, Inc., 2014 WL 3511500 (N.D. Ill. 2014); *In re* Zappos.com, Inc., 108 F. Supp. 3d 949 (D. Nev. 2015); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646 (S.D. Ohio 2014); Green v. eBay No. 14-1688, 2015 U.S. Dist. LEXIS 58047 (E.D. La. May 4, 2014); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014).
[109] Fram, *supra* note 85.
[110] *Id.*; *In re Adobe Sys.*, 66 F. Supp. 3d at 1197; Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).
[111] *In re Adobe Sys., Inc.*, 66 F. Supp. 3d at 1214.
[112] *Id.* at 1211.
[113] *Id.* at 1217.

The court distinguished the facts from *Clapper* by holding that, unlike where hackers already acquire plaintiffs' information, the plaintiffs in *Clapper* could not prove their information was intercepted by the government.[114] Thus, the court held that *Clapper* "presented a risk of harm that was attenuated and speculative and rested on the occurrence of an elongated chain of events."[115]

The greater the likelihood of a third party intervening and breaking the chain of causation, the less likely the court will be to confer standing.[116] Similarly, the court explained the importance of conferring standing for an increased risk of future harm by indicating that "the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach."[117] Consequently, when plaintiffs are forced to wait for the injury to actually occur, defendants use a lack of causation defense to shield themselves from liability. If no injury occurs, plaintiffs are unable to hold companies accountable for breaches to their systems that may cause injury by virtue of the expenses incurred to mitigate the risk of harm.

B. *Application of Clapper Footnote*

In re Adobe relied on the *Clapper* footnote, indicating that the "harm need not already have occurred or be literally certain in order in constitute injury-in-fact."[118] The court held that the footnote supports the proposition that "*Clapper* does not . . . foreclose any use whatsoever of future injuries to support Article III standing . . . [because the Court] did not jettison the 'substantial risk' standard."[119] The substantial risk test was adopted in *Susan B. Anthony List*, holding that the "threat of [a statute's] future enforcement is substantial," and that because the organization challenging the statute's constitutionality faced a "credible threat of enforcement," the plaintiffs met the injury-in-fact requirement.[120] Applying the more lenient substantial risk test allows plaintiffs to establish standing for an increased risk of future injury and is used by courts as an alternative to *Clapper's* heightened standard.[121]

C. *Distinguishing Clapper*

Another notable case distinguishing *Clapper* is *Neiman Marcus*,

[114] *Id.* at 1213.
[115] Sampson, *supra* note 9.
[116] *See In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 957.
[117] *In re Adobe Sys.*, at 1216 n.5.
[118] *Id.* at 1215.
[119] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015)(internal quotations omitted).
[120] Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014).
[121] *Id.*

holding that the future risk of identity or credit card theft was reasonably characterized as real and imminent. The court conferred standing by presuming that the hackers' intention to steal information was to fraudulently misuse that information in the future.[122] In this case, 350,000 credit cards were potentially exposed to malware, which is software intended to damage or disable computer systems.[123] *Neiman Marcus* contacted everyone who shopped at their stores and whose contact information they possessed to offer a year of free credit monitoring and identity-theft protection.[124] Plaintiffs sued on behalf of a class, alleging "negligence, breach of implied contact, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws."[125] Although the plaintiffs had not yet suffered a financial injury or identity theft, they alleged:

> 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information.[126]

Although Neiman Marcus argued that the plaintiffs would be reimbursed for fraudulent charges should they occur, the plaintiffs argued that full reimbursement was not guaranteed.[127] The court acknowledged the risks associated with future injury by reasoning that Neiman Marcus offered credit monitoring services to its consumers because it understood the serious implications of plaintiffs' vulnerability.[128] It distinguished *Clapper*, where plaintiffs lacked evidence that their communications were in fact being monitored. The court also analogized this case to *In re Adobe* by holding that, in both cases, the consumers' information had in fact been stolen, and, thus,

[122] *Remijas*, 794 F.3d at 693.
[123] *Id.* at 690.
[124] *Id.*
[125] *Id.* at 688.
[126] *Id*. at 692.
[127] *Id.*
[128] *Id.*; Kristen Ann Shepard, *Circuit Split on Standing in Data Breach Class Actions Survives Clapper*, CARLTON FIELDS (Sept. 23, 2015), https://www.carltonfields.com/data-breach-class-actions-survives-clapper/.

speculation was unnecessary.[129] As a result, there was an "objectively reasonable likelihood" that future injury would occur.[130]

Where no speculation is required to determine whether the information has in fact been stolen as a direct result of the breach, the court is more likely to distinguish the case from *Clapper*.[131] Nonetheless, despite precedent holding that plaintiffs have standing to sue notwithstanding *Clapper*, plaintiffs must still allege actual monetary damages.[132] The court in *Moyer* held that an increased risk of identity theft, an increased price of goods arising from additional costs incurred by companies to secure financial information, and "additional . . . monetary losses arising from unauthorized bank account withdrawals, fraudulent card payments, and/or related bank fees charged to their accounts" were insufficient to confer standing without actually proving particularized monetary damages.[133]

Moyer held that allegations of monetary losses arising from unauthorized account withdrawals and fraudulent card payments require identifying specific unauthorized withdrawals caused by the breach.[134] The court held that "[d]amages are an essential element of a breach of contract action and a claimant's failure to [plead or] prove damages entitles the defendant to judgment as a matter of law."[135] However, the court held that it may use evidence that one class of plaintiffs suffered fraudulent charges "to substantiate an elevated risk of future injury for the six actual plaintiffs."[136] The court also held that "*Clapper* is distinguishable based on its admittedly rigorous application of the 'certainly impending' standard in a case that involved (1) national security and constitutional issues and (2) no evidence that the relevant risk of harm had ever materialized in similar circumstances."[137] Consequently, it is important to emphasize that although a court may support standing despite *Clapper* based on distinguishable facts, plaintiffs must also prove that the alleged injury is monetary.

D. *Krottner's Credible Threat Standard*

Krottner is a notable case establishing a "credible threat standard," which has been considered a persuasive alternative to *Clapper's*

[129] James M. Westerlind & Andrew Dykens, *Seventh Circuit Again Rules that Victims of a Cybersecurity Breach Have Standing to Sue*, ARENT FOX LLP (June 8, 2016) http://www.lexology.com/library/detail.aspx?g=f079fdcc-b2e9-45d4-9c54-50c6fe043706.
[130] *Remijas*, 794 F.3d at 693.
[131] Moyer v. Michaels Stores, Inc., 2014 WL 3511500, at *6–7 (N.D. Ill. 2014).
[132] *Id.* at 7.
[133] *Id.* at 4.
[134] *Id.* at 7.
[135] *Id.* at 21.
[136] *Id.*
[137] *Id.* at 6 (internal quotations omitted).

"certainly impending" standard.[138] In *Krottner*, a laptop containing plaintiffs' unencrypted personal data was stolen.[139] The court held that the increased risk of future identity theft constituted a credible threat of immediate harm causing plaintiffs to suffer an injury-in-fact by virtue of purchasing expensive services to protect their security.[140] The defendant conceded that "some degree of monitoring [was] an appropriate response" and the court questioned why the defendant would offer plaintiffs a "present remedy" if they had not suffered a "present injury."[141] To conclude that an increased risk of future harm may form the basis to establish standing, the court reasoned that "[a]n injury-in-fact may simply be the fear or anxiety of future harm."[142] Where "emotional and psychological harms" are accompanied by monetary costs that include "preventative steps" associated with the future risk, the showing of injury is only strengthened.[143]

The court in *Krottner* acknowledged that it was unclear whether any one of the 97,000 employees whose information appeared on the laptop would suffer identity theft in the future, or whether the hacker in fact intended to fraudulently use the relevant information.[144] However, the court held that the plaintiffs' fear of information being misused in the future, forcing them to take preventative measures to protect their data, constituted a credible threat "establish[ing] a presently compensable injury."[145]

Courts holding that plaintiffs have standing to sue for future harm are less likely to conflate *Clapper's* "certainly impending" requirement with *Krottner's* "real and immediate" requirement.[146] The court in *In re Sony Gaming Networks*[147] used the "credible threat" test adopted in *Krottner*[148] to conclude that a "credible threat" suffered by a plaintiff is grounds for conferring standing when gaming companies failed to provide adequate network security and comply with industry safeguards

[138] Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).
[139] *Id.* at 1140.
[140] *Id.*
[141] Krottner v. Starbucks Corp., 2009 WL 7382290, at *5 (W.D. Wash. Aug. 14, 2009). ("Starbucks is poorly positioned to argue that there is no credible threat of harm, having already offered these Plaintiffs free credit monitoring.").
[142] *Id.* at 4.
[143] *Id.* at 6 (citing Denney v. Deutsche Bank AG, 443 F.3d 253, 264-65 (2d Cir. 2006))("Binding precedent dictates that Plaintiffs' claims of emotional distress and anxiety arising from the laptop theft are enough to satisfy Article III."); Doe v. Chao, 540 U.S. 614, 617 (2004).
[144] *Id.* ("The allegations show that both Plaintiffs and Starbucks recognize that the threat of identity theft in the wake of the loss of the laptop is not too speculative to constitute an injury in fact.").
[145] *Id.*
[146] Antman v. Uber Techs., Inc., 2015 WL 6123054, at *10–11 (N.D. Cal. Oct. 19, 2015); *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014).
[147] *In re* Sony Gaming Networks, 996 F. Supp. 2d 942 (S.D. Cal. 2014).
[148] Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).

to protect consumer information stored on Sony's network.[149] The court held that *Clapper* did not overrule *Krottner's* "credible threat" test because notwithstanding *Clapper's* "certainly impending" standard, consumers may still suffer a credible threat when their information is stolen.[150]

To the contrary, however, even courts conceding that *Clapper* does not overrule the credible threat test in *Krottner*, hold that because the test requires both a real and immediate credible threat, it "may be interpreted to require the same immediacy of harm that the Supreme Court emphasized in *Clapper*."[151] These courts reason that *Krottner's* real and immediate requirement implies that the injury be certainly impending.[152]

VII. COMPETING INTERPRETATIONS OF *CLAPPER*: CASES REFUSING TO CONFER STANDING FOR INCREASED RISK OF FUTURE INJURY

A. *Application of Clapper's Certainly Impending Standard*

This Note will discuss four prominent cases where the courts, including the Supreme Court, refused to confer standing for allegations of future injury.[153] In *In re Zappos.com*, the plaintiffs alleged that hackers who infiltrated Zappos.com stole their personal information, including their emails, mailing addresses, phone numbers and passwords.[154] The relevant facts distinguishing this case from others that confer standing are that the hackers were only able to view the last four digits of the plaintiffs' credit cards, the plaintiffs waited three and a half years to sue after the breach and they neither alleged that the hackers misused their information nor that their information appeared on the Internet.[155] Additionally, only three of the twelve named plaintiffs incurred expenses, such as credit monitoring services, to mitigate the chance of future harm.[156]

The court held that the plaintiffs' most significant flaw in proving an injury-in-fact was the amount of time that passed between the breach and the lawsuit. This "[undermined] any argument that the threat of harm [was] immediate, impending, or otherwise substantial."[157] The court did not consider the potential for fraud, or the expenses incurred

[149] *In re* Sony Gaming Networks, 996 F. Supp. 2d at 954–55.
[150] *Id.* at 961.
[151] *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 956-57.
[152] *Id.*
[153] *In re Zappos.com*, 108 F. Supp. 3d at 949; Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646 (S.D. Ohio 2014); Green v. eBay No. 14-1688, 2015 U.S. Dist. LEXIS 58047, at *6 (E.D. La. May 4, 2014); Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).
[154] *In re Zappos.com*, 108 F. Supp. 3d at 949.
[155] *Id.*
[156] *Id.* at 953.
[157] *Id.*

by plaintiffs to avoid fraud, as sufficient to confer standing pursuant to *Clapper's* certainly impending requirement.[158] Accordingly, the plaintiffs failed to satisfy the "imminent" requirement of standing.[159] Similar to the holding in *Lujan*, the court held that a credible threat of future harm is insufficient if it is not impending, by stating that "even if the plaintiff faces a real threat, she has no standing until that threat is immediate."[160] Although the court acknowledged that hackers often wait several years before actually using or selling the stolen data, it held that "there must be a point at which a future threat can no longer be considered certainly impending or immediate, despite it still being credible."[161]

The court in *Galaria* also held that plaintiffs failed to meet *Clapper's* "certainly impending" standard.[162] In this case, hackers accumulated plaintiffs' personal information by breaching the system of an insurance company.[163] Due to the costs incurred to mitigate the risk of future harm, a class action ensued alleging violations of the Fair Credit Reporting Act.[164] 15 U.S.C. 1681(b) creates a cause of action for the willful and negligent failure to comply with the statute's requirement "that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit . . . and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality . . . and proper utilization of such information."[165] The defendant conceded that he willfully violated this statute and "offered [plaintiffs] one year of free credit monitoring and identity theft protection" and "suggested that the plaintiffs place a security freeze on their credit reports at their own expense."[166]

Similar to *In re Zappos.com*, the court in *Galaria* held that speculating as to the increased likelihood that the plaintiffs would suffer a future injury in relation to the general public was insufficient to satisfy the real and imminent requirement.[167] The court held that the likelihood of independent actors intervening to cause the injury contributes to the "speculative nature" of plaintiffs' alleged injury.[168] Although the breach

[158] *Id.* at 958.
[159] *Id.*
[160] *Id.* at 959.
[161] *Id.* at 958.
[162] Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014).
[163] *Id.* at 650.
[164] *Id.* at 649.
[165] *Id.* at 652.
[166] *Id.* at 650.
[167] *Id.* at 655.
[168] *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 955; *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C. 2014). ("Finding no standing where plaintiffs allegations of potential identity theft, which had not yet occurred, were "entirely dependent on the actions of an unknown third party").

caused third parties to access their information, whether the plaintiffs suffered an injury-in-fact depended on the criminal conduct of these actors.[169] Moreover, "factual allegation[s] as to how much more likely [the plaintiffs were] to become victims than the general public is not the same as a factual allegation showing how likely they [were] to become victims."[170] The court held that the commonly cited statistic that victims of data breaches are 9.5 times more likely to suffer an actual harm was insufficient to prove the harm was reasonably plausible to satisfy *Clapper's* "certainly impending" standard.[171] They reasoned that "courts view this statistic as evidence of a low absolute risk of becoming a victim of identity theft, even if plaintiffs' relative risk is somewhat higher than the average person's."[172] The court also held that the plaintiffs cannot allege an injury-in-fact based on the costs expended to mitigate the chance of future harm.[173] The court relied heavily on *Clapper* to hold that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that [were] not certainly impending."[174] The reasoning was based on the court's conclusion that the alleged injury was speculative.[175]

B. *Factors to Determine Whether Injury-in-Fact Requirement Satisfied*

In *Green v. eBay Inc.*, eBay suffered a data breach and a lawsuit ensued alleging an increased risk of future identity theft.[176] This case explicitly states important factors the court evaluated in determining whether plaintiffs satisfied the injury-in-fact requirement.[177] These factors included "whether [the plaintiffs'] data was actually taken, when it was accessed, whether certain information was decrypted, whether the data was actually misused or transferred to another third party and misused, and whether or not the third party succeeded in misusing the information."[178] The court held that the plaintiff did not have a substantial enough stake in the outcome of the litigation to satisfy the concrete and particularized standing requirement.[179] The court went so far as to contend that even plaintiffs who suffered fraudulent charges following a data breach may still not have standing if they were not themselves financially responsible for paying the charges.[180] The court

[169] *In re SAIC*, 45 F. Supp. 3d at 26.
[170] Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 654 (S.D. Ohio 2014).
[171] *Id.*
[172] Sampson, *supra* note 9.
[173] *Galaria*, 998 F. Supp. 2d at 657.
[174] *Id.*
[175] *Id.* at 656.
[176] Green v. eBay No. 14-1688, 2015 U.S. Dist. LEXIS 58047, at *1 (E.D. La. May 4, 2014).
[177] *Id.* at *3.
[178] *Id.* at *5.
[179] *Id.*
[180] *Id.*

rejected the argument that hackers' sole purpose in stealing consumers' information is to fraudulently misuse it in the future, holding that it is irrelevant if the future threat of harm is not "certainly impending."[181] This case clearly stands for the proposition that merely alleging that a breach has caused an increased risk of future harm is insufficient to establish standing.[182]

C. *Recent Supreme Court Ruling*

In the 2016 case *Spokeo, Inc. v. Robins*, the Supreme Court reversed a holding granting standing to sue in the data breach context. The Court held that alleged violations of the Fair Credit Reporting Act required not only an individualized but also a concrete injury to satisfy the injury-in-fact requirement of standing.[183] However, the Court's ruling failed to define a concrete injury apart from stating that plaintiffs who enforce rights conferred by statute must only allege the specific harms identified in the statute.[184] Consequently, this ruling failed to definitively conclude whether an increased risk of identity theft is sufficiently concrete and imminent to satisfy the injury-in-fact standing requirement.

D. *Discussion*

My Note will unfold by advocating for three proposals, the combination of which amount to a scheme intended to incentivize companies to improve their cybersecurity policies, which will minimize the prevalence of data breaches and mitigate their impact in the event they occur. First, it will argue that the Supreme Court should compromise between the circuit courts by definitively limiting *Clapper's* "certainly impending" standard to the national security context in which it arose. Consequently, victims of data breaches suing companies for an increased risk of future harm will have standing to hold companies accountable for failing to adequately protect their data. Second, it will argue that Congress should adopt a comprehensive federal statute mandating companies to adopt compliance programs with cybersecurity policies. The extent of the program would vary depending on the company's net income. Third, it will argue that the judiciary should evaluate whether companies have adequately complied with the proposed statute. If, according to an objective good faith standard, companies have reasonably complied, courts should mitigate their damages accordingly. This scheme is designed to encourage companies to adopt appropriate cybersecurity policies that prevent

[181] *Id.*
[182] *Id.* at *6.
[183] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016).
[184] *Id.*

hackers from breaching consumers' security systems with the intention of fraudulently using their personal and financial information.

VIII. LIMITING CLAPPER TO THE NATIONAL SECURITY CONTEXT

To resolve the circuit court split and prevent inconsistency in the data breach context, the Supreme Court should compromise between the circuits conferring standing for an increased risk of future harm on the one hand, and those refusing to confer standing on the other. The Supreme Court can accomplish this by limiting *Clapper's* "certainly impending" standard to cases involving national security threats, such as for plaintiffs alleging violations of § 1881(a).[185] Since the federal government, particularly the legislative and executive branches, is typically responsible for prioritizing national security concerns, separation of powers principles require the standing requirements to be heightened for lawsuits involving this subject matter.[186]

Limiting *Clapper* to the national security context will allow plaintiffs to hold companies accountable, incentivize companies to adopt heightened security measures and help protect against fraud. More plaintiffs would be compensated for injuries by virtue of suffering "the aggravation and loss of value of the time needed to set things straight, reset[ting] payment associations after credit card numbers are changed, and pursu[ing] relief for unauthorized charges"[187] should they occur in the future. These injuries typically involve purchasing credit monitoring and security protection services.[188]

The Court should not limit its characterization of monetary damages to the specific unauthorized withdrawals mandated in *Moyer*.[189] Although unauthorized withdrawals are a well-founded basis for finding that plaintiffs suffered an increased risk of identity theft, the Court should still acknowledge that the financial costs and time-consuming burden of mitigating against the increased risk of future harm is an injury that should be reimbursed in the new digital age. Although *Moyer* acknowledges that "a data security breach and identity theft is not so attenuated that i[t] makes the latter risk speculative or hypothetical,"[190] consumers still suffer an injury despite not yet being the victim of unauthorized payments. If courts wait until the actual harm occurs to grant plaintiffs the opportunity to hold companies accountable, companies will likely be less motivated to implement

[185] Martecchini, *supra* note 1.
[186] *See also* Moyer v. Michaels Stores, Inc., 2014 WL 3511500, at *5 (N.D. Ill. 2014).
[187] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 (7th Cir. 2015).
[188] Rachael Peters, *So You've Been Notified, Now What? The Problem With Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1175–91 (2014).
[189] *Moyer*, 2014 WL 3511500, at *7.
[190] *Id.* at *6.

strategies that mitigate fraud. If companies are not held accountable for monetary harm as a result of data beaches, they may wait until actual harm occurs before they are incentivized to improve their cybersecurity measures.[191]

A. *Conferring Standing to Sue in the Data Breach Context*

Limiting *Clapper* to the national security context would ultimately encourage greater accountability between companies and their consumers. *Clapper* itself does not foreclose the possibility of conferring standing in this way. The aforementioned *Clapper* footnote, validating the use of the "substantial risk test," clearly permits a finding that victims whose information has been stolen and who allege an increased risk of future injury face the substantial risk of future fraud or identify theft.[192] Imposing *Clapper's* heightened standing requirements in the data breach context, whereby plaintiffs are not permitted to sue for an increased risk of future harm, unreasonably disregards the fact that hackers likely breach companies' data systems intending to fraudulently use consumer information for future harm.[193] In fact, according to Verizon's 2016 Data Breach Investigations Report, "89% of breaches had a financial or espionage motive."[194] Moreover, according to a Government Accountability Office Report, "stolen data may be held for up to a year or more before being used to commit identity theft . . . [O]nce stolen data [has] been sold or posted on the Web, fraudulent use of that information may continue for years."[195] This evidence suggests that although plaintiffs have not yet suffered financial harm or identity theft, their increased risk of future injury is still real and imminent despite not being "certainly impending." Therefore, it is important that *Clapper's* standards are limited to the national security context in which they arose.

Allowing plaintiffs to sue for an increased risk of future harm will incentivize companies with lenient data protection to increase their security and sufficiently protect consumer information. Although it must be acknowledged that companies are also the victims of data breaches, allowing plaintiffs to sue companies that fail to protect their data will encourage companies to act proactively rather than refrain

[191] Williams C. Wagner et al., *Cybersecurity: An Affirmative Defense to Ohio Data Breach Negligence Claims*, PRIVACY & DATA SECURITY INSIGHT (Nov 15, 2017), https://www.privacyanddatasecurityinsight.com/2017/11/cybersecurity-an-affirmative-defense-to-ohio-data-breach-negligence-claims/.

[192] Clapper v. Amnesty Int'l U.S.A, 133 S. Ct. 1138, 1150 (2013).

[193] *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014); *Remijas*, 794 F.3d at 693.

[194] *2016 Data Breach Investigations Report*, VERIZON (Feb. 18, 2017 1:16 PM), file:///Users/cristiana/Downloads/rp_DBIR_2016_Report_en_xg.pdf.

[195] U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007).

from acting until a breach occurs. According to a former director of the FBI, "there are only two types of companies: those that have been hacked and those that will be."[196] Especially in recent years, there have been a tremendous amount of cybersecurity attacks leading to consumers suffering either financial harm, identity theft or an increased risk of both in the future.[197] It is counterintuitive that companies can be permitted to wait for breaches and subsequent damage to occur before they are prompted to more efficiently implement procedures that protect consumers' information.

Not only does the circuit court split cause uncertainty and confusion among litigants and lawyers, it also promotes forum shopping, whereby litigants will seek to sue in jurisdictions with more lenient standing requirements that will decide their case on the merits.[198] Consequently, the Supreme Court could encourage consistency by adopting the approach in *In re Adobe* and *Neiman Marcus*, which represents a more pragmatic understanding of hackers' intentions to steal information to fraudulently misuse it in the future.[199] These courts conferred standing on plaintiffs who suffered an increased risk of fraud or identity theft in the future, despite no harm having yet occurred.[200] *In re Adobe* relied on the substantial risk test approved by the *Clapper* footnote to hold that the plaintiffs satisfied the injury-in-fact component of standing because the future risk of financial harm and identity theft posed a substantial risk.[201] *Neiman Marcus* concluded that the plaintiffs satisfied the injury-in-fact component of standing by holding that no speculation is required to infer that the department store offered plaintiffs credit monitoring services because they considered their threat of future injury to be real and imminent.[202]

It is unreasonable that plaintiffs should lack standing to sue because they have not yet suffered an injury that is likely to occur as a result of companies' negligence. Consumers trust companies with their personal and financial information, assuming that they will implement appropriate cybersecurity measures to protect consumer data. As a result, the risk of lawsuit for failure to implement these safeguards will incentivize companies to adopt a serious approach to cybersecurity in practice. The risk of a lawsuit as an incentive for companies to improve their cybersecurity is similar to the incentive provided by the legal safe harbor of the recently proposed Ohio Senate Bill 220. The Bill seeks to

[196] Meyer, *supra* note 3.
[197] King, *supra* note 5; Resnick v. AvMed, Inc., 693 F.3d 1317, 1329 (11th Cir. 2012).
[198] Martecchini, *supra* note 1.
[199] *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).
[200] *In re Adobe Sys.*, 66 F. Supp. 3d at 1216; *Remijas*, 794 F.3d at 693.
[201] *In re Adobe Sys.*, 66 F. Supp. 3d. at 1213, 1217.
[202] *Remijas*, 794 F.3d at 693.

"incentive[ize] businesses to implement certain cybersecurity controls, which can be an affirmative defense to a data breach claim based on negligence."[203] Whether a company believes it will be susceptible to a lawsuit by plaintiffs alleging an increased risk of harm as a result of a data breach, or whether it will be granted an affirmative defense to data breach claims, it will be incentivized to implement reasonable security controls.

The Supreme Court has acknowledged the serious implications of data breaches and an increasing concern for data protection.[204] In *Riley v. California*, the Supreme Court held that police officers were required to obtain Fourth Amendment warrants before inspecting "digital data on the cellphones of arrested suspects."[205] It is inconsistent for the Supreme Court to acknowledge the importance of digital privacy when police officers inspect suspects' cellphones, but fail to take action to protect against fraud likely to occur as a result of data breaches.

B. *Separation of Powers*

Limiting *Clapper* to national security cases brought under 50 U.S.C. §1881(a) not only accommodates the circuit court decisions conferring standing for an increased risk of future harm, but also overcomes many of the legal concerns, namely the separation of powers, that leads the other circuit courts to refuse to confer standing. Permitting the judiciary to decide national security cases on the merits legitimately threatens the separation of powers. For example, conferring standing on plaintiffs alleging an increased risk of future harm resulting from presidential executive orders is more likely to threaten the separation of powers by allowing the judicial branch to encroach on the role of the executive branch. However, the separation of powers is not remotely threatened to the same extent in the data breach context, since the legislative and executive branches are not heavily involved with regulating cybersecurity, as "most major legislative provisions relating to cybersecurity [were] enacted prior to 2002."[206]

Confining *Clapper* to the national security context rather than expanding its reach to limit judicial review in other important contexts is prudent and functional. The threat of the separation of powers in the national security context is much different and more severe than in the data breach context. The Supreme Court acknowledged that the standing doctrine derives from separation of power principles and

[203] Wagner, *supra* note 193.
[204] Riley v. California, 134 S. Ct. 2473 (2014).
[205] *Id.*
[206] Rita Tehan, CONG. RESEARCH SERV., CYBERSECURITY: LEGISLATION, HEARINGS, AND EXECUTIVE BRANCH DOCUMENTS 6 (2017); *see also* Moyer v. Michaels Stores, Inc., 2014 WL 3511500, at *1 (N.D. Ill. 2014); *see also* Martecchini, *supra* note 1.

"[serves] to prevent the judicial process from being used to usurp the powers of the political branches."[207] The judiciary should thus only hear cases or controversies and not assert its opinion in situations that are constitutionally vested in other branches. Applying the standing requirements of a foreign intelligence case, which requires the protections of the separation of powers, to all data breach cases that typically do not involve actions by the legislative or executive branches, unjustifiably limits judicial review and fails to address important concerns posed by data breaches.

The stringent *Clapper* requirements should be limited to national security cases where there is a legitimate risk that courts will unconstitutionally infringe on other branches of government and expand judicial power to issues constitutionally dominated by other political branches. For example, where the lawsuit involves a plaintiff alleging harm as a result of procedures implemented by the executive or legislative branch to combat terrorism at the border or the airport, heightened standing requirements should apply. *Clapper* holds that, "[o]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."[208] Although actions by the legislature, specifically amendments to the Foreign Intelligence Surveillance Act, were at issue in *Clapper*, plaintiffs in the data breach context are not seeking to challenge actions taken by the legislative or executive branch. The plaintiffs are rather seeking to hold companies accountable for insufficiently protecting their data.[209] Accordingly, plaintiffs suing in the data breach context do not pose the same threat to the separation of powers.

Judicial review of the federal legislation proposed by this Note does not infringe on the separation of powers as it would have in *Clapper* if the Court were permitted to review amendments to the Foreign Intelligence Surveillance Act, which were a matter of national security. In *Clapper*, an amendment to the Foreign Intelligence Surveillance Act eliminated certain hurdles that the government had to overcome to obtain permission from the Court to intercept confidential communications.[210] This amendment gave the government significant ability to accomplish its intended surveillance. Plaintiffs in *Clapper* alleged future injury, claiming there was an objectively reasonable likelihood their communications would be intercepted under this

[207] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
[208] Clapper v. Amnesty Int'l U.S.A, 133 S. Ct. 1138, 1141–47 (2013).
[209] Corey Varma, *The Presumption of Injury: Giving Data Breach Victims "A Leg To Stand On"*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 301, 303, 316 (2016).
[210] *Clapper*, 133 S. Ct. at 1144.

amendment.[211] Whereas in *Clapper* the legislature expressed intent to limit judicial review, the legislation proposed by this Note relies on judicial review to ensure companies are complying with the legislation. Moreover, it is indisputably within the constitutional power of the legislature to make law,[212] and within the constitutional power of the judiciary to adjudicate disputes involving allegations of legislative violations.[213]

IX. COMPREHENSIVE FEDERAL STATUTE

Implementing federal cybersecurity legislation is important to provide companies with fair notice of their duties and responsibilities. Without comprehensive legislative guidance establishing uniform cybersecurity policies, the judiciary cannot consistently determine whether companies have implemented reasonable security controls. Federal legislation is also particularly imperative considering "[t]here are no unified federal data-security regulations . . . [and] state breach-notification statutes" vary by state, thus producing "unpredictable and inconsistent" protections.[214] Apart from the Consolidated Appropriations Act, signed into law in 2015, and despite initiatives advanced by President Obama's Administration,[215] the majority of notable cybersecurity provisions were enacted before 2002.[216] The Consolidated Appropriations Act encompasses various components of three information sharing bills: the Protecting Cyber Networks Act (passed by the House), the National Cybersecurity Protection Advancement Act of 2015 (passed by the House) and the Cybersecurity Information Sharing Act of 2015 (passed by the Senate).[217] The Protecting Cyber Networks Act provides liability protection to companies that share security threat information with other companies. The National Cybersecurity Protection Advancement Act protects companies from civil liability when they share their information with the Department of Homeland Security. The Cybersecurity Information Sharing Act provides legal immunity to companies that share their data with the government.[218] Moreover, although President Obama signed five federal cybersecurity bills in 2014, including a bill "codifying the

[211] *Id.* at 1143.
[212] U.S. CONST. art. I, § 1.
[213] U.S. CONST. art. III, § 1; U.S. CONST. art. III, § 2, cl. 1.
[214] Martecchini, *supra* note 1 (citing *Chronology of Data Breaches: Security Breaches 2005 – Present*, PRIVACY RIGHTS CLEARINGHOUSE 94–5 (Apr. 20, 2005), https://www.privacyrights.org/data-breach [perma.cc/TZ9A-SBCR]).
[215] *See FACT SHEET: Cybersecurity National Action Plan*, WHITE HOUSE: OFFICE OF THE PRESS SECRETARY (Feb. 9, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.
[216] Tehan, *supra* note 206, at 1.
[217] *Id.* at 2–3.
[218] Tehan, *supra* note 206, at 6, 8.

role of the National Institute of Standards and Technology (NIST) [to develop] a 'voluntary, industry-led set of standards' to reduce cyber risk,'"[219] they are insufficient on their own to respond to the growing prevalence of data breaches.[220] Congress should adopt more comprehensive legislation mandating companies to implement cybersecurity policies and internal controls as part of their compliance programs. In addition to the legal immunity discussed above, the legislation should outline uniform compliance standards that companies must meet to qualify for mitigated damages when faced with a class action alleging an increased risk of future harm as a result of a data breach.

A. *Cybersecurity Policies*

Congress should adopt legislation establishing uniform cybersecurity policies informed by the expertise of cybersecurity experts who have experience advising companies on appropriate policies. For example, ESET, a Slovakian IT security company recognized for three consecutive years as "Company of the Year,"[221] published guidance on beneficial cybersecurity practices to protect against security threats and malware.[222] Its research determined that smaller businesses, law firms and professional service firms with less than 100 people accounted for 72% of the 855 global data breaches in 2016;[223] these companies spent less on cybersecurity and had "fewer lawyers of protection, less in-house IT expertise, lower levels of awareness, and fewer cybersecurity policies"[224] despite often having more wealth and more valuable data than larger companies. Under the scheme proposed by this Note, the lack of protection would make these companies susceptible to higher damages imposed by the courts in the event of a breach. Higher damages are intended to serve as an incentivizing mechanism that encourages greater protection in the future.

To defend against cyber attacks, the ESET guidance suggests that all companies, regardless of size, should implement compliance

[219] *Id.* (internal quotations omitted).
[220] Joseph Marks, *Obama Took Cyber Seriously and Tried to Tame It, But We're No Safer in Cyberspace Today Than We Were Eight Years Ago, Experts tell Nextgov.*, NETXGOV (Jan. 17, 2017) http://www.nextgov.com/cybersecurity/2017/01/obamas-cyber-legacy-he-did-almost-everything-right-and-it-still-turned-out-wrong/134612/.
[221] *ESET Named "Slovakia's Company of Year" 3rd Time in a Row*, ESET, (Nov. 11, 2010), https://www.eset.com/za/about/press/articles/article/press-eset-named-slovakias-company-of-year-3rd-time-in-a-row/.
[222] Stephen Cobb, *Cybersecurity Policies and Best Practices: Protecting small firms, large firms, and professional services from malware and other cyber-threats*, ESET (Feb. 18, 2017, 1:16 PM), http://www.welivesecurity.com/wp-content/media_files/Cybersecurity-Policy-Small-Firms.pdf.
[223] *Id.*
[224] *Id.* at 9–10; *2016 Data Breach Investigations Report*, *supra* note 194.

programs with established policies.[225] These policies, which should be mandated by the proposed legislation, require automatic updates for antivirus software, prohibiting employees from disengaging the software, scanning all USB drives for viruses, training all employees on how to comply with guidelines, purchasing a secure file transfer system provided by companies such as BISCOM and exclusively using encrypted wireless connections.[226] Moreover, to create cybersecurity policies, ESET recommends that the policy should begin "at the top with buy-in from partners."[227] This means that companies' leadership accepts and is committed to implementing and maintaining appropriate cybersecurity policies as well as encouraging shareholders to support their initiatives. To properly maintain the policies, ESET recommends that "the equipment and software used to process, store, and transmit information be protected by appropriate controls," meaning that companies' privacy policies will be supported in practice by "approved antivirus software [to] be installed on all systems."[228] Furthermore, cybersecurity experts are recently recommending the use of blockchain and its distributed ledger technology as an innovative way to protect against the risks of cybersecurity.[229] The peer-to-peer nature of blockchain "is a method [of] digitally send[ing] something of value without a trusted intermediary or institution," thereby decentralizing the databases it is used on.[230] Blockchain is intended to "[enhance] cybersecurity and the protection of digital assets stored and transferred" by increasing confidentiality. It accomplishes this through the use of irreversible transactions that "prevent the manipulation of databases and thereby reduce fraud."[231]

Although various companies already implement some of these strategies, and many large companies now even mandate law firms to adopt strong policies as a prerequisite to hiring them,[232] a federal statute establishing a reasonable compilation of the aforementioned standards would enhance security and tremendously contribute to uniformity. To account for the fact that not all companies can afford to adopt the same level of protection, the legislation should establish appropriate data protection requirements that correlate with threshold levels of net income. Nonetheless, the legislation should require a minimum level of

[225] Cobb, *supra* note 222; Robbins, *supra* note 100.
[226] Cobb, *supra* note 222, at 18, 24.
[227] *Id.* at 15.
[228] *Id.* at 17.
[229] Jeffrey D. Neuburger & Jonathan P. Mollod, *Blockchain: The Key to True Cybersecurity?*, THE N.Y. L. J. (June 5, 2017), http://www.newyorklawjournal.com/id=1202788075067/Blockchain-The-Key-to-True-Cybersecurity?slreturn=20170513202307.
[230] *Id.*
[231] *Id.*
[232] Cobb, *supra* note 222, at 17.

cybersecurity protection irrespective of net income and financial capacity. The requirements should only vary according to the level of cybersecurity that experts in the field conclude companies with different financial capacities can reasonably afford. For example, small startups and emerging growth companies with modest net income should not be required to adopt procedures as expensive as larger more developed companies.

B. *Compliance Programs*

The federal legislation must also mandate that companies implement compliance programs to internally regulate compliance with the aforementioned cybersecurity policies. The American Bar Association suggests various ways for companies to effectively ensure the proper implementation of cybersecurity policies.[233] It suggests that each company allocate a group of individuals tasked with responding to a data breach, designate specific members of each team to contact in the event of a data breach, and implement immediate mechanisms for preventing the release of further information.[234] It also recommends that all employees, regardless of their position, be well-versed in the company's policies and procedures and be rewarded for complying and penalized for failing to comply.[235] Moreover, all employees should use difficult passwords, invest in firewalls, encrypt data and always track their systems for attacks.[236] The proposed compliance programs should consist of attorneys, outside counsel and public relations teams that help companies implement and comply with self-imposed policies.[237] These policies should strive to ensure companies are complying with the proposed federal legislation. According to the comprehensive scheme proposed, the judiciary would then review companies' compliance with the legislation when plaintiffs allege that the legislation has been breached. Although implementing these strategies may not lead to defendants prevailing on all summary judgment motions, they can certainly aid in mitigating excessive damages.

C. *Safeguarding Against Company Liability*

The purpose of adopting federal legislation that mandates cybersecurity compliance is to prevent data breaches leading to hackers' fraudulent access to consumer information. The purpose of companies implementing internal cybersecurity policies is to help comply with this federal legislation and ultimately mitigate their damages following a

[233] Robbins, *supra* note 100.
[234] *Id.*
[235] *Id.*
[236] *Id.*
[237] *Id.*

data breach. The IBM/Ponemon Data Breach Study estimated that data breaches cost the average company $35 million, while costing larger companies such as Target, Home Depot and Sony anywhere from $15-162 million.[238] These costs are a product of "investigating the breach, repairing compromised systems, notifying victims, providing credit monitoring services to victims, and paying legal fees."[239] Moreover, companies face numerous lawsuits including allegations of "tort, misrepresentation, breach of contract, statutory private rights of action, and invasion of privacy claims."[240] Not only will increased cybersecurity more effectively protect consumer information, it is in companies' best interest to confront security issues to limit their damages.

As certain courts confer standing for an increased risk of future injury and thus defendants' ability to challenge standing has become more difficult, more data breach cases are being decided as a matter of law rather than being remanded to the lower court.[241] Accordingly, for companies to prevail on motions alleging that they "(1) negligently store[d] data, (2) breach[ed] contractual duties to implement cybersecurity, and (3) misrepresent[ed] the effectiveness of their cybersecurity policies," companies must implement proper compliance programs with detailed cybersecurity policies.[242]

In the recent class action against Wells Fargo, where lower-level employees fraudulently opened over two million bank accounts and credit cards "without customers' knowledge or permission," executives were sued for improperly monitoring their employees.[243] A subsidiary of Wells Fargo & Co. was fined $100 million by the Consumer Financial Protection Bureau for opening unauthorized bank accounts.[244] This demonstrates that companies' failure to implement compliance policies and monitor its operations leaves them susceptible to fraud.[245] Although lower-level employees were ultimately responsible for the fraud, the senior executives were liable under agency principles and the respondeat superior doctrine for their failure to implement proper self-

[238] Murgia, *supra* note 4.
[239] *Id.*
[240] *Id.*
[241] *Id.*
[242] *Id.*
[243] Paul Blake, *Wells Fargo Hit With Potential Class-Action Lawsuit After Account Scandals*, ABC NEWS (Sept. 19, 2016), http://abcnews.go.com/Business/wells-fargo-hit-potential-class-action-lawsuit-accounts/story?id=42198894.
[244] Joe Mont, *The Many Compliance Issues of Wells Fargo*, COMPLIANCE WK. (Sept. 20, 2016), https://www.complianceweek.com/news/opinion/the-many-compliance-lessons-of-wells-fargo#.WIgxw7YrK8U.
[245] Henry Engler, *Wells Fargo Case Highlights Need to Monitor Employees with Stressful Performance Goals*, REUTERS: FIN. REG. F. (Sept. 22, 2016), http://blogs.reuters.com/financial-regulatory-forum/2016/09/22/wells-fargo-case-highlights-need-to-monitor-employees-with-stressful-performance-goals-tk/.

policing strategies that ensure their employees' compliance with the law. Although companies are often also the victims of data breaches and are not responsible for infiltrating their own systems, they should be similarly responsible for failing to implement proper compliance programs that ensure conformity with adequate security measures.[246]

Mandating compliance programs through legislation not only ensures that the internal employees of the company are working closely with attorneys to ensure security, but also seeks to manage reputational risks that could damage the company's image. According to a Forbes survey of over 300 companies, managing reputational risks is one of companies' leading concerns to ensure their long-term success.[247] Moreover, permitting victims of these breaches to seek redress through the judiciary will prompt companies to adopt appropriate compliance measures that encourage executives to pay closer attention to their employees' actions.

D. *Counterarguments to Federal Legislation*

In a concurrence in *Riley v. California*, Justice Alito, who wrote the *Clapper* opinion, advocated for a federal statute addressing data breaches.[248] The lack of Congressional guidance addressing liability for data breaches further perpetuates the circuit split.[249] Nonetheless, a counterargument to this proposal is that, although theoretically useful, it may not be easily invoked in practice, as "disagreements between Republicans and Democrats in Congress have blocked proposed federal legislation addressing data breach issues."[250] However, now that the Senate and the House of Representatives are both Republican, deadlocks are much less likely.[251] Moreover, "[d]espite the lack of enactment of cybersecurity legislation in the 112th Congress [whereby the bill failed to secure two votes], there still appears to be considerable support in principle for significant legislation to address [cybersecurity] issues."[252]

Although Republicans may be hesitant to excessively regulate companies, the Russian cyber invasion during the presidential election,

---

[246] Robbins, *supra* note 100.

[247] 2014 Global Survey on Reputation Risk, DELOITTE (Jan. 26, 2017, 6:05 PM), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf.

248 Riley v. California, 134 S. Ct. 2473, 2497 (2014).

[249] Clara Kim, Note, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2016 COLUM. BUS. L. REV. 544, 573–76 (2016).

[250] *Id.*

[251] Richard Cowan & Susan Cornwell, *Republicans defend grip on U.S. Congress as Trump wins presidency*, REUTERS (Nov. 9, 2016, 1:24 PM), http://www.reuters.com/article/us-usa-election-congress-idUSKBN13317Z.

[252] Tehan, *supra* note 206, at 1.

confirmed by the testimony of "[t]op U.S. intelligence officials . . . at a hearing on cybersecurity threats,"[253] is one of many instances exemplifying the serious implications of failing to address cybersecurity.[254] According to "interviews with dozens of players targeted in the attack, intelligence officials who investigated it[,] and President Obama administration officials who deliberated over the best response[, the attack can be attributed to] a series of missed signals, slow responses and a continuing underestimation of the seriousness of the cyberattack."[255] Although the failure to internalize the scope and severity of the attacks "undercut efforts to minimize their impact[,]" the White House's ability "to respond forcefully [in the future]. . . could prove critical in deterring future cyberattacks."[256] The fact that even the Democratic National Committee's system was vulnerable to attack at an imperative time demonstrates the need to continually monitor and update cybersecurity systems in response to the increasingly sophisticated tactics employed by hackers.[257]

X. JUDICIAL APPLICATION OF FEDERAL STATUTE

The proposed federal legislation relies on collaboration between the legislature and the judiciary by requiring the judiciary to evaluate companies' compliance with cybersecurity policies mandated by the legislation. It would be counterintuitive for Congress to adopt legislation governing cybersecurity if the courts could not determine when it was violated. Allowing plaintiffs who suffer an increased risk of future harm to sue companies following a data breach further incentivizes companies to abide by the legislation in fear of litigation.

Conferring standing on plaintiffs alleging an increased risk of future harm following a data breach primarily accommodates the circuit courts that have conferred standing on this basis in the past. However, the proposed scheme also seeks to compromise with the other circuit courts that refuse to confer standing on plaintiffs alleging an increased risk of future harm, holding they do not suffer a "certainly impending" injury as a result of companies' negligence. To compromise with these circuit courts, not only should the Supreme Court confer standing on plaintiffs suing companies that fail to protect their data, they should also mitigate companies' damages if companies prove their compliance with

[253] Watch: Full Senate hearing on Russian hacking and US cybersecurity, PRI (Jan. 5, 2017), https://www.pri.org/stories/2017-01-05/watch-live-senate-hearing-russian-hacking-and-us-cybersecurity.
[254] Eric Lipton, David E. Sanger & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.
[255] *Id.*
[256] *Id.*
[257] *Id.*

the proposed legislation. To evaluate a company's compliance with the proposed legislation, courts should compare the company's compliance program and its cybersecurity policies with the legislative requirements governing companies with the same net income threshold. Courts should apply the legislation consistently to all companies depending on net worth. They should also consider that companies often do not intentionally allow hackers to access consumer information and, thus, they are also the victims of data breaches.[258] Consequently, when deciding whether or how much to mitigate companies' damages, courts should consider companies' objective good faith effort to mitigate security breaches through compliance programs with effective cybersecurity policies. They can do this by considering whether companies have reasonable justifications for why they suffered a breach despite reasonable efforts to implement safeguards. Rewarding companies that make an objective good faith effort to comply with the proposed legislation by implementing sufficient cybersecurity policies will incentivize companies to protect consumer data in the new digital age.[259]

Companies must protect consumer data by implementing compliance programs that enhance security and mitigate the risks of data breaches and the expensive litigation that results. Companies must be vigilant in upgrading their security, as the methods used in cyber attacks have become increasingly sophisticated. Only when companies can prove to the courts that they have sought to adequately ensure security and protect consumer information should their damages be mitigated. Mitigating damages for companies that demonstrate a good faith effort to establish proper security standards will encourage businesses to implement these programs in practice. As data breaches and the fraud that ensues have become extremely prevalent today, and as companies are in the best position to mitigate security violations, implementing compliance programs is crucial to ensure increased security through self-policing. As is expressed by Arent Fox LLP, a law firm representing large companies against their risk of lawsuit, "[h]aving a written data security incident policy and written procedures for responding to an actual or suspected data security incident is a must."[260] Motivating companies to limit the risk of cyber attacks will help protect them against allegations that plaintiffs suffer concrete and imminent harm as a result of costs incurred to mitigate against the

[258] *See* Nick Hopkins, *Deloitte Hit by Cyber-Attack Revealing Clients' Secret Emails*, GUARDIAN (Sept. 25, 2017, 8:00 AM), https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails.
[259] Wagner, *supra* note 191.
[260] Westerlind & Dykens, *supra* note 129.

increased risk of future harm.[261]

CONCLUSION

The inconsistent circuit court rulings in the data breach context, specifically, those refusing to confer standing on plaintiffs suing companies for an increased risk of future harm, perpetuate the prevalence of data breaches in recent years.[262] When plaintiffs are unable to hold companies accountable for their data breaches, companies lack the necessary incentives to invest in proper security protection. This issue is further exacerbated by the lack of comprehensive federal legislation mandating companies to implement compliance programs with reasonable cybersecurity policies. Prompting companies to improve their security requires the Supreme Court to resolve the circuit court split by accommodating for approaches adopted by both sides.

The Supreme Court can compromise between the circuit court rulings by limiting *Clapper's* "certainly impending" standard to the national security context.[263] This would increase the chance of conferring standing for allegations of an increased risk of future harm in the data breach context. To create a uniform standard permitting companies to understand their obligations and avoid litigation in the data breach context, Congress should enact federal legislation mandating corporate cybersecurity policies, whereby the breadth of the policies vary according to companies' net income. This would empower courts to consistently review companies' compliance.[264] When companies prove compliance with the legislation based on an objective good faith standard, courts should mitigate their damages accordingly. This scheme enables companies to internalize the costs of litigation arising from potential liability, provides compensation to data breach victims that incur expenses to mitigate against future harm and incentivizes companies to improve their cybersecurity protection.

Cristiana Modesti[*]

[261] *Id.*
[262] *See* Martecchini, *supra* note 1.
[263] *Id.*
[264] Kim, *supra* note 249.

[*] J.D., Benjamin N. Cardozo School of Law, 2018. B.A., Queen's University, 2015. I would like to thank my parents for their unconditional love and support.