Standing in the Aftermath of a Data Breach

Ariel Emmanuel*

ABSTRACT

This Article analyzes the potential redress individuals have against entities that allow personally identifiable information to be exposed in a data breach. For an individual to bring a case of increased risk of identity theft against such an entity, an individual must establish standing, which requires a showing of injury. However, federal courts have not ruled uniformly as to whether an increased risk of identity theft—due to such breach—is a cognizable injury for standing purposes. Recently, the U.S. Supreme Court in Clapper v. Amnesty Int'l USA applied a "certainly impending" standard for cases wherein a plaintiff based all claims on an increased risk of a future injury. Even though a small minority of lower courts have applied this standard, a large degree of confusion in this area of law remains, given that different jurisdictions still produce disparate outcomes when examining analogous facts.

This Article seeks to reject the application of the "certainly impending" standard in the increased risk identity theft context since the context in which Clapper was decided—holding a federal statute relating to national security unconstitutional—is fundamentally different from

* Ariel Emmanuel is a third year law student at the Emory University School of Law in Atlanta, GA. Ariel holds a B.S. in Accounting & Finance from Florida State University and is a native of Miami, FL.

the context of finding an increased risk of identity theft. Furthermore, Clapper should not be applied in the increased risk of identity theft context because the injury in Clapper was more speculative than the average identity theft case. In contrast, this Article employs the more lenient standard used in other Supreme Court cases whose facts are more similar to the increased risk of identity theft cases to create a new standard. This Article will use this new standard to propose a resolution for the Circuit split. This Article will further address the limit to this new standard and situations where standing would not be condoned.

INTRODUCTION

Consider this situation: you are normally a vigilant person and very cautious in safeguarding your identity. However, you learn that your personal information may have been compromised after receiving a letter from your favorite retailer regarding a recently experienced data breach. With the ever looming threat of identity theft, how do you respond? Does the law provide any redress for you against this retailer for its inadequate security network?

Identity theft has become an epidemic problem in society today.[1] Every day news media seem to report about another corporate entity that has experienced a hack or about a family member whose identity was unexpectedly stolen.[2] As a

---

[1] IDENTITY THEFT VICTIMS STATISTICS, http://www.identitytheft.info/victims.aspx (last visited Jan. 7, 2015).

[2] Nicole Perlroth, *Kmart and Dairy Queen Report Data Breach*, N.Y. TIMES BITS BLOG (Oct. 10, 2014, 7:46 PM),

result, "approximately fifteen million U.S. residents have their identities used fraudulently each year with financial losses totaling upwards of $50 billion."[3] Identity theft is defined by the Bureau of Justice Statistics as "the unauthorized use or attempted use of existing accounts, or the unauthorized use or attempted use of personal information to open a new account or for other fraudulent purposes."[4]

Hacking into the computer systems and networks of large entities is one of the most fruitful methods of obtaining individuals' information because such criminal actors can obtain information from a large number of individuals from a single source.[5] About one in four individuals whose information is leaked in a corporation's data breach will subsequently suffer identity theft.[6] The retail industry is the most-frequented target for such hackers, followed closely by the financial services

---

http://bits.blogs.nytimes.com/2014/10/10/kmart-and-dairy-queen-report-data-breach/.

[3] IDENTITY THEFT VICTIMS STATISTICS, http://www.identitytheft.info/victims.aspx (last visited Jan. 7, 2015).

[4] Ericka Harrell, Ph.D. and Lynn Langton, Ph.D., *Victims Of Identity Theft, 2012*, BUREAU OF JUSTICE STATISTICS (Dec. 12, 2013), http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821.

[5] *E.g.* Jessica Silver-Greenberg, Matthew Goldstein and Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES, Oct. 2, 2014, http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_r=0.

[6] Ann Carrns, *The Cost to Consumers of a Data Breach*, N.Y. TIMES BUCKS BLOG (Apr. 30, 2013, 11:15 AM), http://bucks.blogs.nytimes.com/2013/04/30/the-cost-to-consumers-of-a-data-breach/.

industry and health care companies.[7] Social security numbers are the most common form of information stolen because of their inherent commercial value on the black market.[8]

Data breaches have been increasing each year around the country. In California for example, California's Attorney General reported that 167 data breaches were reported in the State in 2013—a 28% increase from the 131 data breaches reported in 2012.[9] Further, for the first ten months of 2014, breaches in California were up thirty percent from 2013.[10] This increase in data breaches resulted in the information of more than 18.5 million California residents being compromised in 2013.[11] The Attorney General reported that most of this increase in data breaches was the result of the use of newer technologies leaving information more vulnerable to individuals with malicious intentions.[12] Likewise, in New York, there were more than 900 data breaches in 2013, exposing the personal and financial records of 7.3 million New Yorkers to theft.[13] New York's Attorney General, in

---

[7] Nicole Perlroth, *Report Analyzes Extent of Data Breaches in California*, N.Y. TIMES BITS BLOG (Oct. 28, 2014, 1:00 PM), http://bits.blogs.nytimes.com/2014/10/28/report-analyzes-extent-of-data-breaches-in-california/.

[8] *Id.* ("the average amount of fraud caused by a single Social Security number is $2,330 compared with $2,026 for a debit card and $1,251 for a stolen credit card.").

[9] Perlroth, *supra*, note 7.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] Mike Isaac, *Data Breaches in New York Hit Record High in 2013, State Attorney General Says*, N.Y. TIMES BITS BLOG (July 15, 2014, 12:01 AM), http://bits.blogs.nytimes.com/2014/07/15/attorney-general-

fact, believes that many of these breaches could have been prevented.[14]

Overall, the amount of data breaches and the number of individuals affected has become more prevalent in our society.[15] With the resulting increased risk of identity theft these individuals face,[16] many of them hope to receive redress from the courts.

A victim of a data breach must principally rely on a theory of an increased risk of identity theft in order to recover.[17] The first step in a case of an increased risk of identity theft is the plaintiff must prove that he/she has standing to bring the claim.[18] Establishing standing is especially difficult in examining the context of an increased risk of identity theft, given the Circuit split between the Seventh, Ninth and Third Circuits.[19] The Seventh and Ninth Circuits allow standing for an increased

---

says-new-york-had-more-than-900-data-breaches-in-2013/?_r=0.

[14] *Id.*

[15] *See* paragraph above. Some of the more recent incidents of data breaches include the Target breach, which affected forty million individuals, and the Home Depot breach, which affected sixty million individuals.

[16] *See* Carrns, *supra* note 6. Nicole Perlroth, *Home Depot Data Breach Could Be the Largest Yet*, N.Y. TIMES BITS BLOG, (Sep. 8, 2014, 6:58 PM), http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/.

[17] The theory of an increased risk of identity theft is mainly used in claims where the plaintiff is seeking damages for emotional distress, time, and energy spent reversing unauthorized charges and/or protecting against future fraud. *See e.g.*, Anderson v. Hannaford Bros. Co., 659 F.3d 151, 155 (1st Cir. 2011).

[18] *See* Allen v. Wright, 468 U.S. 737, 750 (1984).

[19] *Infra* note 20

risk of identity theft, while the Third Circuit precludes standing in this context.[20]

Although it is unlikely that the Supreme Court will take up the increased risk of identity theft issue,[21] the Court has recently decided the issue of whether an increased risk of injury constitutes compensable damages in *Clapper v. Amnesty Int'l USA*. In *Clapper*, the Court applied a "certainly impending" standard,[22] which is one of the strictest standards the Court has ever applied.[23] Several district courts have employed the holding from *Clapper* to propose a resolution for this Circuit split on the increased risk of identity theft issue.[24] These decisions stood for the proposition that *Pisciotta* and *Krottner* are overruled and standing should not be allowed in most increased risk of identity theft cases.[25]

This Article rejects the standard from *Clapper* as a resolution for the Circuit split between the Third Circuit—which does not allow standing

---

[20] *Compare* Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010), *and* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007), *with* Reilly v. Ceridian Corp., 664 F.3d 38 (3rd Cir. 2011) (The courts in *Krottner* and *Pisciotta* allowed their respective cases to proceed while the court in *Reilly* denied standing because the risk of injury was not "certainly impending.").

[21] *See, e.g.*, *Reilly*, 664 F.3d 38, *cert. denied*, 132 S. Ct. 2395 (2012). Furthermore, the issue of whether an increased risk of identity theft alone is sufficient to establish standing has not recently been decided by any U.S. Court of Appeals.

[22] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

[23] *See infra* note 200.

[24] *E.g.* Galaria v. Nationwide Mut. Ins. Co., 998 F.Supp.2d 646 (S.D. Ohio 2014).

[25] Strautins v. Trustwave Holdings, Inc., No. 12 C 09115, 2014 WL 960816, at *5 (N.D. Ill. Mar. 12, 2014).

for an increased risk of identity theft claim—and the Seventh and Ninth Circuits—which do allow standing for such claims. Although other scholarship has discussed standing in data breach cases, this Article can be contrasted.[26]

This Article proposes that the courts should look towards other Supreme Court cases in which the facts are more similar to the increased risk of identity theft context, and employ the holdings from those cases to formulate a new standard for the increased risk of identity theft context. Part I of this Article will provide the legal background for standing doctrine. This Part begins with a general

---

[26] *See, e.g.*, Patricia Cave, Comment, *Giving Consumers a Leg to Stand on: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. REV. 765 (2013) (Discussing the issues in the area of standing in data breach cases, but proposes that the solution to this issue should come from Congress); Miles L. Galbraith, Comment, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365 (2013) (Proposing a resolution to this issue using settled principles in tort law. This Comment analogizes defective medical device, toxic substance exposure, and environmental injury cases with data breach cases to find that standing should be allowed in the latter cases); John L. Jacobus & Benjamin B. Watson, *Clapper v. Amnesty International and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?*, 21 Rich. J.L. & Tech. 3 (2014) (summarizing the current state of the laws surrounding standing in data breach cases, fails to suggest a solution to the issue); Lexi Rubow, Comment*, Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKELEY TECH. L.J. 1007 (2014) (Comparing *Clapper* with *Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010), to propose a more relaxed standard to privacy cases based on a unique view of the injury-in-fact requirement.).

discussion of standing, then continues with a discussion of standing within the context of an increased risk of identity theft. Part I then presents a history of the case law to show how it developed, how the judiciary's views on identity theft advanced, and the ways it impacted the development of the modern day Circuit split.[27] Part II of this Article will then analyze the effects of *Clapper* on the standard for finding standing in increased risk of identity theft cases. This Part discredits *Clapper* in the increased risk of identity theft context and proposes a new, more relaxed, standard based on the standards used in other Supreme Court cases that are more applicable to increased risk of identity theft. Part III then addresses looming criticisms and the implications of a more relaxed standard.

I. BACKGROUND

This Part of the Article begins with an exploration the requirements of Article III standing. Section A begins with a discussion of the rudimentary requirements of standing, and Section B describes the development of jurisprudence on standing in increased risk of identity theft cases, eventually leading up to the Circuit split. Afterwards, this Part will go into a discussion of *Clapper* and the "certainly impending" standard. This Part concludes with an exploration of post-*Clapper* cases discussing standing in the increased risk of identity theft context. These cases illustrate the insufficiency of the guidance *Clapper* provided to lower courts in navigating this area of law.

---

[27] *See infra*, Part I, Section B, Subsection 1.

A. *THE JURISPRUDENCE OF STANDING*

Before a discussion of standing in the identity theft context can proceed, it is necessary to establish a background by discussing standing in general. Article III of the Constitution "confines the federal courts to adjudicating actual 'cases' and 'controversies.'"[28] "One element of the case-or-controversy requirement of Article III standing is that plaintiffs must establish that they have standing to sue."[29]

Standing, as explained in *Allen v. Wright*, requires three essential components: 1) there must be an injury that is "distinct and palpable" and not "abstract" or "conjectural" or "hypothetical";[30] 2) "such injury must be 'fairly' traceable to the challenged action"; and 3) the injury must be likely to be redressed from a favorable ruling of the

---

[28] Allen v. Wright, 468 U.S. 737, 750 (1984). This doctrine is based on the concept of separation of powers, and provides that courts should be limited to only their constitutionally defined roles. *Id.* (citing to Valley Forge Christian College v. Americans United for Separation of Church and State, Inc., 454 U.S. 464, 471–76 (1982) *and* Warth v. Seldin, 422 U.S. 490, 98 (1975)); *See also* U.S. CONST. art. III. A fundamental principle of the judiciary's role in this separation of powers is that they be limited in this way. *Clapper*, 133 S. Ct. 1138 (citing DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006).

[29] *Clapper*, 133 S. Ct. 1138.

[30] Allen v. Wright, 468 U.S. at 751 (citing Gladstone, Realtors v. Village of Bellwood, 441 U.S. 91, 100 (1979), L.A. v. Lyons, 461 U.S. 95, 101–102 (1983) *and* O'Shea v. Littleton, 414 U.S. 488, 494 (1974)).

case.[31] Because the U.S. Constitution does not provide an analysis of standing, the meanings of these three amorphous requirements have been largely defined by case law.[32]

Additionally, standing doctrine embraces several court-made limitations on standing.[33] These "prudential" limits on the power of the courts require: 1) there not be a claim on behalf of a third party;[34] 2) a claim not be a generalized grievance;[35] 3) and "that a plaintiff's complaint fall within the zone of interests protected by the law invoked."[36] These prudential limits are beyond the scope of this Article because the constitutional requirements are the core components of establishing standing.[37]

B. *STANDING IN THE INCREASED RISK OF IDENTITY THEFT CONTEXT*

Identity theft is the misappropriation of an individual's personal information for the purpose of fraud or other crimes.[38] When the identity theft is

---

[31] Allen v. Wright, 468 U.S. at 751 (citing Valley Forge Christian College v. Americans United for Separation of Church and State, Inc., 454 U.S. 464, 474–75 (1982)).
[32] *See id.* at 751–52. *See* U.S. CONST., art. III.
[33] Allen v. Wright, 468 U.S. at 750–51.
[34] *Id.*
[35] *Id.* (these issues are more appropriately addressed by the legislative branch of the government).
[36] *Id.*
[37] *See* Allen v. Wright, 468 U.S. at 751; *see* Lexmark International, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377, 1386–88 (2014) (although *Lexmark* abrogates the holding of *Allen v. Wright*, this only relates to the rule about prudential standing, so Lexmark also need not be mentioned in this article).
[38] Galper v. JP Morgan Chase Bank, N.A., No. 14–0867–cv, 2015 WL 5711882, at *1 (2d Cir. Sept. 20, 2015).

caused by another party's negligence in securing the identity theft victim's information, then the victim has a claim against that negligent party.[39] The more difficult question is in the situation where a person's information was stolen due to the negligence of another party, but the person has not suffered from identity theft. The question is whether the person has standing to bring a case against the negligent party based on the increase in the future risk of suffering from identity theft.

1. The Direction of the Early Jurisprudence

The jurisprudential origins of standing in increased risk of identity theft cases have largely denied standing. One of the earlier cases, *Stollenwerk v. Tri-West Healthcare Alliance*,[40] set the precedent for increased risk of identity theft claims by denying standing.[41] In *Stollenwerk*, the facility of a healthcare company was burglarized twice and the hard drives from the computers at that facility were stolen.[42] One of the plaintiffs suffered from identity theft after the burglaries.[43] The court in *Stollenwerk* rejected standing for the plaintiffs who claimed an increased risk of identity theft.[44]

---

[39] *See* Resnick v. AvMed, Inc., 693 F.3d 1317, 1323 – 24 (11th Cir. 2012).
[40] Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906, at *1 (D. Ariz. Sept. 6, 2005).
[41] Many cases cited to *Stollenwerk*, and many other cases cited to rulings from this case.
[42] *Id.* (the hard drives contained the personal information of Tri-West Healthcare's clients).
[43] *Id.*
[44] *Id.*

The court distinguished toxic tort and medical monitoring cases from identity theft cases to find that the former cases involve a latent injury at the time of the exposure, the public interest of supporting medical monitoring after exposure is greater than the interest of supporting credit monitoring, and identity theft can be compensated after the fact, which eliminates the need for credit monitoring.[45] The court determined that there was neither evidence that the information was actually stolen nor evidence of an increased risk of identity theft.[46]

The next year, the District Court for the Southern District of Ohio in *Key v. DSW* relied partly on *Stollenwerk* to establish its view that the injury in the increased risk of identity theft context must be "actual or imminent."[47] In denying standing the court found that the "Plaintiff's claims [were] based on nothing more than a speculation that she will be a victim of wrongdoing at some unidentified point in the indefinite future."[48]

Stollenwerk and *Key* were important in forming the requirements for establishing standing in the increased risk of identity theft context. Many other cases decided during this period relied on the precedent of *Stollenwerk* and *Key*. Nonetheless, towards the late 2000s, jurisprudence began to reflect a liberal interpretation of harm and a Circuit

---

[45] *Id.* at *3.
[46] *Id.* at *5; *Aff'd in part*, 254 Fed. Appx. 664, 665–67 (9th Cir. 2007).
[47] Key v. DSW, Inc., 454 F.Supp.2d 684, 689 (S.D. Ohio 2006).
[48] *Id.* at 690.

split developed between the Seventh and Ninths Circuits and the Third Circuit.[49]

2. The Circuit Split

a. The Seventh Circuit allowing Standing

In 2007, the Seventh Circuit in *Pisciotta v. Old National Bancorp* rejected the earlier cases[50] to find that an increased risk of identity theft is a sufficient injury to allow standing.[51] In *Pisciotta*, the defendant learned of a security breach in its hosting facility in which "the scope and manner of access suggest[ed] that the intrusion was sophisticated, intentional and malicious."[52] There, two potential customers filed a class action arguing that the defendant's negligence exposed them to an increased risk of a third party misusing their information.[53]

In its analysis, the Seventh Circuit considered cases both from jurisdictions which do not allow standing for an increased risk of identity

---

[49] Miles L. Galbraith, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1365–66 (2013).

[50] These cases including *Stollenwerk*, 2005 WL 2465906, in the District of Arizona and *Hendricks v. DSW Shoe Warehouse*, 444 F.Supp.2d 775, 783 (W.D.Mich 2006).

[51] *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007).

[52] *Id.* at 631–32 (the defendant provided banking services and required their customers to fill out applications disclosing their "name, address, social security number, driver's license, number, date of birth, mother's maiden name and credit card or other financial account numbers.").

[53] *See id.*

theft,[54] as well as cases from jurisdictions which allow standing for an increased risk of future harm in other contexts, including toxic tort, medical monitoring and environmental claims.[55] From the latter cases, the court in *Pisciotta* found that once a person has been exposed to the negligence of the defendant, injury-in-fact is met if a substantial risk can be found that a plaintiff would suffer from harm in the future.[56] The court in *Pisciotta* concluded that an increased risk of identity theft is a sufficient basis for standing because the risk of injury has increased.[57] The holding in *Pisciotta* marked a turning point in standing jurisprudence, with an increasing amount of courts willing to find standing for an increased risk of identity theft.[58]

b. The Ninth Circuit Allowing Standing

[54] *See id.* at 634 n.2 (citing Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 10 (D.D.C. 2007); Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006); Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006); Giordano v. Wachovia Securities, LLC, No. 06-476 (JBS), 2006 WL 2177036, at *5 (D.N.J. July 31, 2006).

[55] *See Pisciotta*, 499 F.3d at 634 n.3 (citing Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2nd Cir. 2006); Sutton v. St. Jude Medical S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005); Central Delta Water Agency v. U.S., 306 F.3d 938, 947–48 (9th Cir. 2002); Friends of the Earth, Inc. v. Gaston Cooper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000)).

[56] *See Pisciotta*, 499 F.3d at 634.

[57] *Id.*

[58] *See* Galbraith, *supra* note 49, 1382 (citing McLoughlin v. People's United Bank, Inc., No. 3:08-cv-00944, 2009 WL 2843269 (D. Conn. Aug. 31, 2009) and New York in Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273 (S.D.N.Y. 2008)).

In 2010, the Ninth Circuit in *Krottner v. Starbucks Corp.* relied partly on *Pisciotta* to establish standing for a claim of an increased risk of identity theft.[59] In *Krottner*, a laptop containing the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees was stolen from Starbucks.[60] Less than two months after the breach, one of the employees alleged that his bank had notified him of an attempt to open an account in his name.[61] Him, and two other employees filed identical class action complaints against Starbucks alleging negligence and breach of implied contract.[62]

The court in *Krottner* looked towards other contexts, such as environmental and medical monitoring claims, and other Circuits for a solution.[63] From the different contexts, the court found that the plaintiff must be in immediate danger of suffering from the alleged harm, and the "threat of injury is both real and immediate, not conjectural or hypothetical."[64] The court then discussed *Pisciotta* and the Seventh Circuit's analysis and ultimate holding that an increased risk of future harm is sufficient to impose standing.[65] The Ninth Circuit in *Krottner* found increased risk of identity

[59] Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).
[60] *Id.* at 1140 (the opinion does not indicate how the laptop was stolen).
[61] *Id.* at 1141.
[62] *Id.*
[63] *Id.* at 1142.
[64] *Id.* (citing Scott v. Pasadena United School District, 306 F.3d 646, 656 (9th Cir. 2002) (this standard has been applied to the context of environmental claims and medical monitoring claims).
[65] *Krottner*, 628 F.3d at 1142–43.

theft sufficient to establish standing because such a plaintiff had faced a "credible threat of harm," which was "both real an immediate, not conjectural or hypothetical."[66]

c. The Third Circuit Denying Standing

In 2010, the Third Circuit in *Reilly v. Ceridian Corp.* rejected both *Pisciotta* and *Krottner* to find that an increased risk of identity theft is insufficient to establish standing.[67] In this case, Ceridian Corp., a payroll processing firm, suffered a security breach when "[a]n unknown hacker infiltrated [its] Powerpay system and potentially gained access to personal and financial information belonging to . . . approximately 27,000 employees at 1,900 companies."[68] The victims of this data breach sued, claiming they had suffered an increased risk of identity theft.[69]

The court considered the requirements of Article III standing and found that "allegations of 'possible future injuries' are not sufficient to satisfy

---

[66] *Krottner*, 628 F.3d at 1143 (the threat was "credible" and "immediate" because the laptop with the plaintiffs "unencrypted personal data" was stolen. The court mentioned that the claim would be less credible and imminent if the laptops were not stolen and the plaintiffs were only suing on the fear that the laptops would be stolen in the future.).
[67] Reilly v. Ceridian Corp., 664 F.3d 38 (3rd Cir. 2011).
[68] *Id.* at 40. (the personal and financial information may include the employee's names, addresses, social security numbers, dates of birth, and bank account information.).
[69] *Id.*

Article III.'"[70] The injury must be "certainly impending" and "proceed with a high degree of immediacy, so as to reduce the possibility of deciding a case in which no injury would have occurred at all."[71] Considering the facts at bar, the court in *Reilly* found the plaintiffs relied on speculation of whether a hacker actually would misuse their personal information.[72] Crucial to the court's determination, however, was the uncertainty of future events: only if an event happens in the future will the plaintiff suffer from an injury.[73] Because no evidence was presented at trial to suggest the plaintiff's information had been misused, one would have to speculate that the information would be misused in the future.[74]

The court then considered the plaintiff's comparison to *Pisciotta* and *Krottner* as grounds for a grant of standing.[75] But the court distinguished those two cases from the facts in *Reilly* because no evidence had been presented in *Reilly* to demonstrate that the intrusion was intentional or malicious.[76] The court in *Reilly* stated that because the breaches in *Pisciotta* and *Krottner* were

---

[70] *Id.* at 41–42 (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990); Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 n.2 (1992)).
[71] *Id.*
[72] *See id.* (the court compared this case with *Lujan*, 504 U.S. at 564 n.2, where plaintiff visiting the project sites at some time in the future was speculative; and City of Los Angeles v. Lyons, 461 U.S. 95 (1983), where although the plaintiff experienced a chokehold in the past, it was speculative whether he would be subject to one in the future).
[73] *Id.*
[74] *Id.* at 43.
[75] *Id.*
[76] *Id.* at 44.

intentional and malicious, the possible injuries were more "imminent" and "certainly impending" than the possible injury in *Reilly*.[77]

Further, the court in *Reilly* rejected the application of the standards used in defective-medical-device, toxic-substance exposure, and environmental-injury cases because they are fundamentally different than increased risk of identity theft cases.[78] The court in *Reilly* further distinguished medical device and toxic tort cases because in those cases, the plaintiff suffers an actual injury and there are quantifiable damages in the future. The court also noted that for policy reasons, those type of cases are different since they involve health and the balance between life and death is in question. Then considering environmental cases, the court stated that one cannot wait for the harm to the environment to occur, because at that point, compensation would not do anything; e.g. extinction of an animal species, destruction of wilderness, etc.[79] The court therefore declined to confer standing because the injury alleged was not imminent.[80]

3. *The Strict Standard in Clapper*

The U.S. Supreme Court has never directly addressed the issue of standing in the increased risk

---

[77] *Id.*
[78] *Id.* at 44–46; *Pisciotta*, 499 F.3d at 634; *Krottner*, 628 F.3d at 1142–43.
[79] *Id.*
[80] *Reilly*, 664 F.3d at 46. *But see* Ceridian Corp., 151 F.T.C. 514 (2011) (where the Federal Trade Commission finds Ceridian Corp. in violation of the Federal Trade Commission Act in a separate adjudication related to the same breach.).

of identity theft context, yet in 2013, in *Clapper v. Amnesty Int'l USA*, the Court considered the standard for recognizing standing for a future injury.[81] This is important to the analysis because several subsequent increased risk of identity theft cases have relied on *Clapper*.

Clapper is about the amendment to the Foreign Intelligence Surveillance Act of 1978 ("FISA") which allows the surveillance of certain individuals located outside the U.S.[82] The respondents were several individuals and organizations who filed suit claiming that the amendment was unconstitutional.[83] The respondents claimed that their communications with foreign contacts would be intercepted sometime in the future under FISA and its amendment.[84]

With regard to standing, the respondents argued their communications with foreign contacts would be intercepted sometime in the future under FISA and its amendment.[85] The Court rejected this argument on the grounds that the "objectively reasonable likelihood" standard that the respondents were arguing was inconsistent with its previous holding of the injury being "certainly impending."[86]

---

[81] *Clapper*, 133 S. Ct. 1138 (The holding from *Clapper* is important to the analysis of this Article because subsequent to this decision, many increased risk of identity theft cases used *Clapper* for guidance of what is the correct standard for standing.).
[82] *Id.* at 1140.
[83] *Id.*
[84] *Id.* at 1145–47 (their contacts were people the Government "believes or believed to be associated with terrorist organizations," in geographical areas that were of particular attention to the Government.).
[85] *Id.* at 1147.
[86] *Id.*

The Court then explained that the injury the respondents alleged was not "certainly impending" due to the fact that it depended on the possibility of future events—the occurrence of which was only speculative.[87] Providing a speculative chain of events that must happen before an injury can occur, as opposed to concrete evidence that the injury will occur, does not support standing.[88] In effect, the Court concluded that the injury must be "certainly impending" for standing to be established.[89]

4. The Post-Clapper Jurisprudence

Subsequent jurisprudence to the *Clapper* decision addressing standing in an increased risk of identity theft context has shown no consistent trend.[90]

---

[87] *Id.* at 1148 (the events required for the respondents' injury to materialize are: "(1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under §1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy §1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.").

[88] *Id.* at 1154.

[89] *Id.* at 1155 (furthermore, any costs incurred to avoid those injuries do not establish standing if the "certainly impending" standard has not been met.).

[90] *Compare In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., No. 12-347 (JEB), 2014 WL 1858458 (D.D.C. May 9, 2014), Remijas v. Neiman Marcus Croup, LLC, No. 14 C 1735, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014), Strautins v. Trustwave Holdings, Inc., No. 12 C 09115,

In early 2014, the Southern District of Ohio in *Galaria v. Nationwide Mutual Insurance Co.* relied upon *Clapper* to deny standing plaintiff claiming an increased risk of identity theft.[91] In *Galaria*, a breach occurred at Nationwide Mutual Insurance Co. ("Nationwide"); [92] during the breach, thieves hacked into Nationwide's system, then stole and disseminated the personal identifiable information of Nationwide's customers.[93] A class of individuals whose information was hacked during this breach sued Nationwide claiming their injury was an increased risk of identity theft.[94] The court in *Galaria* cited *Clapper* finding both that the standard for a claim of a future injury must be "certainly impending" and "[a]llegations of possible future injury are not sufficient."[95] The court states that the injury is even more speculative when it requires the actions of a third party.[96] The court went on to note that *Clapper* overruled *Krottner* and

---

2014 WL 960816 (N.D. Ill. Mar. 12, 2014), Galaria v. Nationwide Mut. Ins. Co., 998 F.Supp.2d 646 (S.D. Ohio 2014), *and* Lewert v. P.F. Chang's China Bistro, Inc., No. 14-cv-4787, 2014 WL 7005097 (N.D. Ill. Dec. 10, 2014), *with In re* Adobe Sys., Inc. Privacy Litig., Case No.: 13-CV-05226-LHK, 2014 WL 4379916 (D. San Jose Sept. 4, 2014), Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014), *and In re* Sony Gaming Networks and Customer Data Sec. Breach Litig., 996 F.Supp.2d 942 (S.D. Cal. 2014).

[91] Galaria v. Nationwide Mut. Ins. Co., 998 F.Supp.2d 646 (S.D. Ohio 2014).

[92] *Id.* at 649–50.

[93] *Id.*

[94] *Id.* at 649–51.

[95] *Id.* (citing to *Clapper*, 133 S.Ct. at 1146).

[96] *Id.* at 655.

Pisciotta.[97] In employing the "certainly impending" standard, the court found that plaintiffs did not have standing on their increased risk of identity theft claim because their injury was not "certainly impending."[98]

But since *Clapper* was decided, the cases of increased risk of identity theft have not uniformly agreed with *Clapper* to reject standing.[99] There have been several opinions that have either disagreed with *Clapper* or disagreed that *Clapper* heightened the standard for standing in increased risk of identity theft cases.[100]

In 2014, the Ninth Circuit in *in re Sony Gaming Networks and Customer Data Sec. Breach Litig.* allowed standing for a claim of an increased risk of identity theft after the court's consideration of *Clapper*.[101] This case involved several of Sony's online services being hacked and the personal information of millions of its users being stolen.[102] Users are required to provide to Sony their personal

---

[97] *Id.* at 655–56 (the court stated that it is possible for standing to be found in the increased risk of identity theft context, but does not cite to any cases it believes satisfied this standard or any court it believed got it correct in finding a plaintiff had standing).

[98] *Id.* at 657.

[99] *See supra*, note 90. More recently, a U.S. District Court judge in Minnesota allowed standing for the individuals whose information was exposed in the Target data breach in their lawsuit against Target. Reuters, *Consumers Can Sue Target Corp Over Data Breach: Judge*, N.Y. TIMES, Dec. 19, 2014, http://www.nytimes.com/reuters/2014/12/19/business/19reuters-target-breach-lawsuit.html.

[100] *See infra* note 101.

[101] *In re* Sony Gaming Networks and Customer Data Sec. Breach Litig., 996 F.Supp.2d 942 (S.D. Cal. 2014).

[102] *Id.* at 954–55.

identifying information, including their names, mailing addresses, email addresses, birth dates, credit and debit card information, and login credentials.[103] In analyzing whether plaintiffs had standing to bring a claim of increased risk of identity theft due to the breach, the court in *Sony* considered whether it should continue to apply the decision of *Krottner* in light of the *Clapper* decision.[104] Ultimately, the court in *Sony* rejected the argument that *Clapper* heightened the injury-in-fact requirement.[105] It distinguished *Clapper* because in *Clapper*, the "respondents failed to sufficiently allege Article III standing because a speculative chain of possibilities based on potential future surveillance was not enough to plausibly allege a 'certainly impending' injury."[106] But in *Krottner*, standing was found "based on a 'credible threat of harm' that was 'both real and immediate, not conjectural or hypothetical.'"[107] The Supreme Court did not overrule its previous requirements that harm be "real and immediate."[108] Thus, in applying both *Krottner* and *Clapper*, the court in *Sony* found standing based on the plaintiff's

---

[103] *Id.* at 954.
[104] *Id.* at 960–61 (*Krottner* is the precedent in the Ninth Circuit).
[105] *Id.* at 961.
[106] *Id.*; *see Clapper*, 133 S. Ct. at 1150 (there were five event that had to occur before the injury could materialize, and some of these events were speculative in and of themselves).
[107] *Sony*, 996 F.Supp.2d at 961; *see Krottner*, 628 F.3d at 1143 (there was a stolen laptop containing the plaintiff's information, and less than two months later, somebody attempted to open a bank account using one of the plaintiff's information.).
[108] *Sony*, 996 F.Supp.2d at 961.

allegation that his information was collected and improperly disclosed as a result of the breach.[109]

In summary, case law to date does not create a clear rule as to whether a person whose information was disclosed in a data breach would be able to recover on the theory of an increased risk of identity theft because of the Circuit split. Furthermore, the method of applying *Clapper* to the increased risk of identity context remains unclear since different courts interpret *Clapper* in different ways.[110] Therefore it is necessary to reinterpret the case law and draw out a rule for determining standing in the increased risk of identity theft context that is legally supported, achieves the desired policy outcomes, and can be consistently applied.

II. THE STANDARD FOR INCREASED RISK OF IDENTITY THEFT

This Part of the Article analyzes the "certainly impending" standard from *Clapper*, and proposes a more suitable standard for increased risk of identity theft cases. Section A explores *Clapper*'s effects on the Circuits and the difficulties the Circuit split has created in defining a standard for identity theft cases. Section B then addresses how *Clapper* is inappropriate for use in the identity theft context. This Section further analyzes the different standards the Supreme Court has used in the context of future injuries, and the appropriateness of each

---

[109] *Id.* at 961–62 (the court employs several cases to back up this proposition that an allegation that the information was collected and wrongfully disclosed is sufficient to impose standing).

[110] *See supra*, note 90.

for the identity theft context. Section C then discusses the creation of a new, more relaxed standard to apply in increased risk of identity theft cases, with Subsection 1 explaining how this new standard is defined, and Subsection 2 applying this new standard to the cases in the Circuit split, highlighting the unavoidable difficulties of a more relaxed standard.

A. *CLAPPER'S EFFECT ON THE FEDERAL CIRCUIT COURT DECISIONS*

There exists an unresolved Circuit split between the third Circuit and the seventh and ninth Circuits as a result of the opinions from *Pisciotta*, *Krottner*, and *Reilly*. Although the *Reilly* court attempts to explain why the facts in its case are distinguishable from those of in *Pisciotta* and *Krottner*, the *Reilly* court *also* fundamentally disagrees with the holding of the other two cases.[111]

The court in *Reilly* began its analysis with the contention that an increased risk of identity theft cannot confer standing.[112] However, faced with the *Pisciotta* and *Krottner* cases, in which standing was established in the increased risk of identity theft context, the court in *Reilly* claimed the cases were not persuasive because their facts were distinguishable and not because their holdings were unsupported or erroneous.[113] The *Reilly* court distinguished its facts by stating that there was no evidence that the intrusion was intentional or malicious while the breaches in both *Pisiotta* and

[111] *Reilly*, 664 F.3d at 41–46.
[112] *Id.* at 41.
[113] *Id.* at 43–45.

Krottner were intentionally done by third parties with malicious intent.[114] [115]

The analysis by the *Reilly* court is flawed[116] because the exposure of information after a data breach does in fact increase the risk the individuals will suffer from identity theft.[117] The court stands for the proposition that a claim of an increased risk of identity theft is insufficient to support standing because an increase in risk does not guarantee that the event would occur.[118] The proposition that *Reilly* relies on is that the risk of injury must be certain to happen in order for standing to be established.[119] This is much higher than the standard employed by *Pisciotta* and *Krottner*. The court in *Reilly* found that the breach was unintentional,[120] but larger scale security breaches,

---

[114] *Id.* at 44; *Pisciotta*, 499 F.3d at 632; *Krottner*, 628 F.3d at 1141.

[115] *Reilly*, 664 F.3d at 44. But whether the facts in *Reilly* is that different from those in *Pisciotta* and *Krottner* is debatable. Glenn Lammi, *Federal Circuit Court Goes Its Own Way on Standing in Data Security Class Action*, WLF LEGAL PULSE, Jan. 6, 2012, http://wlflegalpulse.com/2012/01/06/federal-circuit-court-goes-its-own-way-on-standing-in-data-security-class-action/

[116] *See* Galbraith, *supra* note 49, 1387–88.

[117] *See* Carrns *supra*, note 6 (one in four victims of data breaches will suffer from identity theft).

[118] *See Reilly*, 664 F.3d at 43.

[119] *See id.* at 42 (The court reasoned that "[u]nless and until" the steps preceding the injury materialized, there is no injury or harm.).

[120] The record in *Reilly* did not include the fact that the hackers executed a "Structured Query Language" ("SQL") injection attack on the Powerpay System and web application. Ceridian Corp., 151 F.T.C. 514, 528 (2011); *see Reilly*, 664 F.3d 38. The hackers found the personal information stored on the system and exported this information. *Id.*

like the one in *Reilly*, are usually intentional.[121] Therefore, the court in *Reilly* essentially disagreed with the holdings of the other two Circuits and reaffirmed its view that an increased risk of identity theft cannot establish standing.[122] But it asserted that it was distinguishing the facts in its case from the facts of the other two cases.[123]

There are serious jurisprudential problems associated with an existing Circuit split in this arena. These problems include the difficulty other courts will face as the result of the lack of a uniform and clear standard.[124] Further, splits create unnecessary litigation because attorneys from jurisdictions where it had already been decided may try to argue that their precedent should be overturned looking at the emerging vision of the other jurisdictions.[125]

One way to resolve the problems associated with the Circuit split is to identify a new, broadly

---

[121] *See In re Adobe Sys., Inc. Privacy Litig.*, 2014 WL 4379916 at *9 (the court contemplates few purposes of a security breach other than to misuse the information gathered). Even if the hackers in *Reilly* did not know how to utilize the information obtained, there is a vast Black Market for this kind of information, where it—especially the financial information—could have been sold to third parties. Tom Zeller, Jr., *Black Market in Stolen Credit Card Data Thrives on Internet*, N.Y. TIMES, June 21, 2005, http://www.nytimes.com/2005/06/21/technology/21data.html

[122] *See Reilly*, 664 F.3d at 41–46.

[123] *See id.*

[124] *See generally* Wayne A. Logan, *Constitutional Cacophony: Federal Circuit Splits and the Fourth Amendment*, 65 Vand. L. Rev. 1137 (2012).

[125] *See* Joseph C. Pettygrove, *Circuit Court's Split Over Prounion Law May Have Consequences for Employers*, 17 No. 2 IND. EMP. L. LETTER 5 (2007) (analyzing circuit split in the employment context).

applicable standard. The first step in defining a new standard is finding the similarities between the cases and Circuits. In *Pisciotta*, there was a breach of the hosting facility that maintained a bank's website.[126] In *Krottner*, a laptop containing employees' information was stolen.[127] These cases are factually analogous in that they both involve an intentional act by a third party,[128] as opposed to the mere exposure of information by a company.[129] Likewise, the third party in both cases was a thief and/or a person with malicious intentions.[130] Thus, in both cases, a third party gained access to the plaintiff's personal information, and there was a high probability that such individuals would use the stolen information to the plaintiff's detriment.[131] Although the court in *Reilly* arrived at a different

---

[126] *Pisciotta*, 499 F.3d at 632.
[127] *Krottner*, 628 F.3d 1141.
[128] *Pisciotta*, 499 F.3d at 631–32; *Krottner*, 628 F.3d at 1140–41.
[129] *See* Katz v. Pershing*, LLC*, 672 F.3d 64, 70, 80 (1st Cir. 2012) (Where the plaintiff claimed the company made the plaintiff's information available publicly on the internet, but had not claimed that a third party had accessed it).
[130] *See id.*
[131] *See id.* (Furthermore, in *Krottner*, somebody actually did use the plaintiff's information in a malicious manner since less than two months after the theft, somebody attempted to open a bank account using the social security number of one of the plaintiffs); *see* Ann Carrns, *Protecting Yourself After a Data Breach*, N.Y. TIMES, June 6, 2013, http://bucks.blogs.nytimes.com/2013/06/06/protecting-yourself-after-a-data-breach/ (the main use of information in a data breach is for fraud purposes.); *but see* Brooke Barnes and Nicole Perlroth, *Sony Films are Pirated, and Hackers Leak Studio Salaries*, N.Y. TIMES, Dec. 2, 2014, http://www.nytimes.com/2014/12/03/business/media/sony-is-again-target-of-hackers.html (a minority of data breaches are used to embarrass the company).

conclusion as to whether such plaintiffs have standing, the facts in *Reilly* are substantially similar to that of *Krottner* and *Pisciotta*.[132] *Reilly* involved a breach of the database of a payroll processing firm.[133] The breach in *Reilly* was likely intentional because the facts surrounding the breach are indicative of an intentional third party act.[134] But there was little evidence presented in *Reilly* to show that the breach was for a malicious purpose.[135] That was the critical issue in that case that resulted in the court denying standing for the plaintiffs.

The application of *Clapper* makes the analysis more challenging because of the strict standard derived from it. [136] But *Clapper* can still be contrasted from the increased risk of identity theft cases because of its facts and context. Because *Pisciotta* and *Krottner* both granted standing, the facts must be compared to decide whether those two cases would have come out the same under the precedent of *Clapper*. The alleged injury in *Clapper* involved too many hypothetical steps,[137] and was too attenuated.[138] As a result, the injury in *Clapper* was deemed not to be "certainly impending," and standing was denied.[139] Yet, the injuries alleged in both *Pisciotta* and *Krottner* were less hypothetical than the one in *Clapper*. In *Pisciotta*, the only events required before the injury could materialize is that the identity thief had to obtain the personal

---

[132] *See Reilly*, *supra* notes 119–123.
[133] *Reilly*, 664 F.3d at 40.
[134] *See supra*, note 121.
[135] *See Reilly*, 664 F.3d at 40, 44.
[136] *See Clapper*, 133 S. Ct. at 1141.
[137] *Id.* at 1151.
[138] *Id.* at 1148.
[139] *Id.* at 1155.

identifiable information, use that information and not get caught.[140] The injury in *Krottner* was even less attenuated than that in *Pisciotta* because there was evidence that a third party possessed the personal identifiable information, so the only event that had to occur was the third party use that information in a malicious manner.[141] This second step of not getting caught in *Krottner* was a little more speculative because one attempt to use the plaintiff's information had already been stopped.[142]

There still may be too many steps in *Pisciotta* and *Krottner*, causing the risk of injury to be too attenuated using the "certainly impending" standard.[143] The court in *Reilly* on the other hand distinguished the facts before it from the aforementioned, and concluded that an increased risk cannot support standing.[144] To establish standing, *Clapper* requires sufficient evidence to show that an injury will in fact occur.[145] Accordingly, if the standard from *Clapper* were applied to the facts in *Reilly*, *Pisciotta* and *Krottner*, it is doubtful that standing would have been established in any of these cases. Standing would have been denied because in all three cases, the injuries were too speculative because they were premised on the independent acts of third parties to

---

[140] *Pisciotta*, 499 F.3d at 632, 639–40 (the information was already obtained by malicious means, so somebody already had the information, and therefore, these are the most logical steps afterwards).
[141] *Krottner*, 628 F.3d at 1140–41.
[142] *Id.* at 1141.
[143] *See Clapper*, 113 S. Ct. at 1150.
[144] *Reilly*, 664 F.3d at 44–46.
[145] *See Clapper*, 113 S. Ct. at 1146–50.

occur at some unforeseeable time in the future.[146] The Court in *Clapper* specifically rejected the idea that an injury is "certainly impending" if there is only an "objectively reasonable likelihood" the injury will occur.[147]

B. *SUPREME COURT'S PRECEDENT ON STANDING*

The "certainly impending" standard applied in *Clapper* is one of the strictest standards for finding standing available in case law.[148] It essentially requires a party seeking to establish standing to present sufficient evidence to show that the injury *will* in fact occur at a *definite* point in the future.[149] This standard is based on the viewpoint that the judiciary is only allowed to hear cases where an injury has happened or will definitely happen, but has yet to materialize.[150] Courts allow recovery in the latter situations only because a plaintiff should not—as a matter of public policy—have to wait to get injured to be allowed to recover

---

[146] *Clapper*, 133 S. Ct. at 1141; *in re Adobe Sys., Inc. Privacy Litig.*, 2014 WL 4379916, *7 n.4 (the use of "certainly impending" in the Supreme Court can be traced back to 1923 with Pennsylvania v. West Virginia, 262 U.S. 553, 593 (1923), and has been cited in several Supreme Court cases since then).

[147] *Clapper*, 133 S. Ct. at 1147.

[148] *See, e.g., infra*, note 200.

[149] *Clapper*, 133 S. Ct. at 1160 (Breyer, J., Dissenting) (emphasis added); *See also in re Adobe Sys., Inc. Privacy Litig.*, 2014 WL 4379916, at *7 (citing *Clapper*, 133 S. Ct. at 1150 n.5) (implying that the "certainly impending" standard means that the injury *will* occur in the future) (emphasis added).

[150] *See id.*

when they already know they will be injured in the future.[151]

However, the "certainly impending" standard is not the only viable standard for courts to apply.[152] The Supreme Court has applied several different standards in determining whether standing should be allowed in future harm cases,[153] ranging from the very strict[154] to the lenient.[155] The Court has discretion as to what standard to apply, and it has usually been fact and context specific.[156] In light of this discretion, the "certainly impending" standard from *Clapper* is not the most appropriate standard to apply in increased risk of identity theft cases.

1. Why Clapper Should Not Apply in Increased Risk of Identity Theft Cases

In cases where the injury is based on an increased risk of identity theft, the standard of proof should not be as strict as the "certainly impending" standard used in *Clapper*. There are two justifications for this. First, the facts in *Clapper* are far more attenuated and speculative than the average increased risk of identity theft case. Second, the context in which *Clapper* was decided, declaring the Foreign Intelligence Surveillance Act

---

[151] *See* Pennsylvania v. West Virginia, 262 U.S. 553, 593 (1923).
[152] *See* discussion *infra*, XXXX.
[153] *See infra*, note 200.
[154] *Lujan*, 504 U.S. at 563–64.
[155] Davis v. Federal Election Commission, 554 U.S. 724, 734 (2008).
[156] *See infra* note 199.

unconstitutional, is fundamentally different than the context of increased risk of identity theft. The "certainly impending" standard is therefore not the most appropriate for increased risk of identity theft cases.

a. The Facts in Clapper were too Attenuated and Speculative

Under the "certainly impending" standard in *Clapper*, the sequence of events must neither be "too attenuated," nor "too speculative."[157] The Court in *Clapper* did not allow standing because the facts and circumstances of that case failed to meet the two requirements.[158] However, this often is not the case in in the average identity theft case. It would therefore be better to apply a standard from the less attenuated/speculative cases.[159]

The average increased risk of identity theft case has less attenuated circumstances than those in *Clapper*. In a data breach situation, there is evidence that another party already has the information, and the only subsequent step required is that the person use that information in a malicious manner.[160] *Krottner*, for example, involved the theft of a laptop and a subsequent attempt to use the plaintiff's information to open an

---

[157] *Clapper*, 133 S. Ct. at 1147.
[158] *Id.* at 1148.
[159] *See Moyer*, 2014 WL 3511500, at *5
[160] *See* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014) (the chain of causation connecting a data security breach and identity theft is not as attenuated as that presented in *Clapper*, so is therefore not as speculative and hypothetical).

account.[161] *Pisciotta* involved a "sophisticated, intentional and malicious" breach of a database.[162] *Reilly* involved the breach of a payroll processing firm's data, which was likely to be intentional.[163] In all three cases, the information was inappropriately acquired, and the only additional step required was the use of the information. Most plaintiffs in identity theft cases find themselves in this situation.[164] This is far from the several steps required for the injury in *Clapper* to materialize. Increased risk of identity theft cases are better compared to cases where there were fewer steps required before the injury could occur.[165]

Attempting to avoid speculation presents another issue because in the context of an identity theft case, there must be speculation regarding two things: 1) that another person has the information, and 2) that the person would use the information in a malicious way.[166] Rarely is there evidence that both of these events are certain and will definitely happen, so both are usually partially based on speculation. The question is: how speculative is too speculative in the case of an increased risk of identity theft?

The facts in *Krottner* require little speculation that the injury would eventually

---

[161] *Krottner*, 628 F.3d at 1140–41.
[162] *Pisciotta*, 499 F.3d at 632.
[163] *See Reilly*, 664 F.3d at 40; *see supra*, note 121.
[164] *See, e.g.*, Nicole Perlroth, *Who Is Selling Target's Data?*, N.Y. TIMES BITS BLOG, (Dec. 24, 2013, 7:52 PM), http://bits.blogs.nytimes.com/2013/12/24/who-is-selling-targets-data/.
[165] *See infra*, Part II, Section C, Subsection 1; Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153 n.3 (2010).
[166] *Reilly*, 664 F.3d at 42.

occur.[167] When analyzing the first step in *Krottner*, there is little speculation required because a laptop with the information on it was stolen.[168] Accordingly, is was known that somebody had the laptop.[169] It would therefore require little speculation to conclude that someone would have taken from the laptop the personal information contained therein.[170] Although it is possible the laptop came into the hands of someone with no interest in the information,[171] it is more likely that the person who stole the laptop accessed the information.[172]

The facts in *Pisciotta*, similar to those in *Krottner*, also require little speculation.[173] One does not need to speculate because "the scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious."[174] An intentional intrusion is indicative of somebody wanting the information, and because the

---

[167] *Krottner*, 628 F.3d 1139.
[168] *Id.* at 1140–41.
[169] *See id.*
[170] *See id.*
[171] It is possible that the person that stole the laptop only wanted the physical value of the laptop rather than the value of the information on the laptop. In that case, there is a possibility that the person that stole the laptop sold it to a totally innocent person, who had absolutely no interest in doing something malicious with this information.
[172] *See* Lisa W. Foderaro, *Stolen Laptops Helps Turn Tables on Suspects*, N.Y. TIMES, May 10, 2008, http://www.nytimes.com/2008/05/10/nyregion/10laptop.html
[173] *Pisciotta*, 499 F.3d 629.
[174] *Id.* at 632; *see* Ann Carrns, *Protecting Yourself After a Data Breach*, N.Y. TIMES BUCKS BLOG (June 6, 2013, 12:49 PM), http://bucks.blogs.nytimes.com/2013/06/06/protecting-yourself-after-a-data-breach/ (the main purpose of data breach is to utilize the information for fraud purposes.).

information was actually taken, the hacker was successful in the goal of obtaining the information.[175] So the facts in *Pisciotta* require little speculation that someone had obtained the information. Among *Pisciotta*, *Krottner* and *Reilly*, facts in *Reilly* require the most speculation about the first step of cases of increased risk of identity theft. All that is known in *Reilly* is that there was a breach of the firewall.[176] It is unknown whether any of the information was actually stolen.[177] But based on the facts and surrounding circumstances, it is likely that the breach was intentional.[178] Therefore, the only further speculation required was whether the hacker was successful in obtaining the information. Although the facts in *Reilly* required more speculation than *Krottner* and *Pisciotta*, it is not clear that the facts are so dissimilar as to suggest that standing should have been found in *Pisciotta* and *Krottner*, but not in *Reilly*.

The second step of speculation in cases of increased risk of identity theft is whether the information accessed will be used to the detriment of the plaintiff. Limited speculation is required to conclude that the information will be used for improper purposes if there is a preliminary conclusion that the information was accessed.[179] Personal information, especially in large quantities, has great commercial value due to the ease of employing the information to commit identity theft

---

[175] *See Pisciotta*, 499 F.3d at 632.
[176] *Reilly*, 664 F.3d at 40.
[177] *Id.*
[178] *See id.*; *see supra*, note 121.
[179] *In re Adobe Sys., Inc. Privacy Litig.*, 2014 WL 4379916 at *9 (". . . after all, why would hackers target and steal personal customer data if not to misuse it?"); *see* Carrns, *supra*, note 6.

for personal gain.[180] Even if the person in possession of the information does not have the ability to utilize the information for identity theft, that person can easily sell the information on the vast underground market for personal information.[181]

Due to the variety of things that the person can do with the information and the ease with which they can do it, it requires little speculation that somebody would subsequently utilize the information.[182] Returning to the issues in the Circuit split, *Krottner* required even less speculation than the average data breach case because somebody already attempted to use one of the plaintiff's information for malicious purposes.[183] Because an attempt to use the plaintiff's information already occurred in *Krottner*, there was a high probability of it happening again.[184] Thus, it requires little speculation to conclude that someone would subsequently use the information.[185] *Pisciotta* and *Reilly* are more similar to the typical case, so taking the first step as true, it requires little speculation as to whether somebody in possession of the stolen information would eventually use the information in some malicious way.[186]

Overall, there is little speculation required in these cases—*Piciotta*, *Krottner*, and *Reilly*—which

---

[180] *See supra*, note 5.
[181] *Id.*
[182] *See supra*, note 6 (One in four victims of a data breach will in fact become victims of identity theft).
[183] *Krottner*, 628 F.3d at 1141 (the attempt of opening the bank account in the plaintiff's name.).
[184] *See Reilly*, 664 F.3d at 44 (discussing the breach in *Krottner*).
[185] *Id.*
[186] *Pisciotta*, 499 F.3d at 631–32; *Reilly*, 664 F.3d at 40.

is far different from the speculative events in *Clapper*.[187] For the injury in *Clapper* to materialize, the Government would have to specifically target the individuals the plaintiffs communicate with.[188] The injury also would have required the government to use its authority under the statute in question, as opposed to the numerous other authorized methods of surveillance at the Government's disposal.[189] Furthermore, it is unclear whether the government would succeed in acquiring the communications of its targets and that they would intercept the particular communications between the targets and the plaintiffs.[190] Because these facts in *Clapper* require far more speculation than the facts in identity theft cases such as *Krottner*, *Pisciotta* or *Reilly*, there is justification for using a different standard for standing in identity theft cases than the standard employed in *Clapper*. Applying the higher standard from *Clapper* would be inappropriate in the identity theft context because of the fundamental difference in the speculation required for each type of cases.

b. The Unique Context of Clapper

The second justification for not applying the certainly impending standard in identity theft cases is because the context in *Clapper*, declaring the Foreign Intelligence Surveillance Act unconstitutional, is fundamentally different from the context of an increased risk of identity theft.

---

[187] *See Clapper*, 133 S.Ct. at 1147–50.
[188] *See id.* at 1148–49.
[189] *See id.* at 1149.
[190] *See id.* at 1150.

"*Clapper*'s discussion of standing arose in the sensitive context of a claim that other branches of government were violating the Constitution, and the Supreme Court itself noted that its standing analysis was unusually rigorous as a result."[191] Yet, *Clapper* left open the question of whether its standard should apply in cases that neither present national security nor constitutional issues.[192]

The standard from *Clapper* should not apply because allowing the *Clapper* plaintiffs to proceed could have affected our national security or led to the invalidation of an act of Congress.[193] Each of those could have severe repercussions.[194] The Supreme Court did not want to proceed unless it was certain that the plaintiff had suffered some kind of injury. By contrast, with identity theft cases, allowing the case to proceed could result in a company being held liable for the repercussions of its negligence in permitting a data breach. The ramifications of an identity theft case are not as consequential as a constitutional or national security case. Thus, a plaintiff should be held to a less demanding standard in proceedings of an increased risk of identity theft cases brought within the context of a data breach.[195]

---

[191] *In re Adobe Sys., Inc. Privacy Litig.*, 2014 WL 4379916, at *7 (citing *Clapper*, 133 S. Ct. at 1147 ("Our 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.")).
[192] *Moyer*, 2014 WL 3511500, at *5 (citing Strautins v. Trustwave Holdings, Inc., No. 12 C 09115, 2014 WL 960816, at *5, n.11 (N.D. Ill. Mar. 12, 2014)).
[193] *Id.*
[194] *Id.*
[195] *See Moyer*, 2014 WL 3511500, at *5.

Accordingly, courts deciding whether to allow standing in increased risk of identity theft cases should not apply the "certainly impending" standard in *Clapper*. Courts should instead seek guidance from other Supreme Court cases whose facts and contexts are more similar to these of the increased risk of identity theft cases.[196]

2. Consideration of Other Supreme Court Cases

Courts should apply a less stringent standard than "certainly impending" in analyzing whether standing should be recognized in every case of an increased risk of identity theft. This inflexible standard as currently applied denies recovery to many legitimate claimants, leaving many potential identity theft victims with no form of recourse. Although "certainly impending" as a standard for standing has existed for decades,[197] the dissent in *Clapper* correctly noted that the Court has used many different terms over the years to describe the standard required for standing.[198] Other terms used by the Court terms have applied a lower standard for certainty of harm than in *Clapper*.[199] The range of these terms include:

> "'reasonable probability' that suggest less than absolute, or literal certainty,"

---

[196] Courts must look towards similar cases since the Supreme Court has not directly addressed the issue of an increased risk of identity theft.
[197] *See* Babbit v. United Farm Workers Nat'l Union, 442 U.S. 289, 298 (1979).
[198] *Clapper*, 133 S. Ct. at 1160–61 (Breyer, J., Dissenting).
[199] *E.g.* Blum v. Yaretsky, 457 U.S. 991 (1982).

> . . . "a *realistic danger* of sustaining a direct injury," . . . "the defendant's allegedly wrongful behavior will likely occur or continue," . . . "'reasonable probability' and 'substantial risk,'" . . . "realistic and impending threat of direct injury," . . . "genuine threat of enforcement," . . . "substantial likely," . . . "sufficient likelihood of economic injury," . . . "realistic danger," . . . "'quite realistic' threat," . . . "likely," "reasonable probability."[200]

The Supreme Court fails to use one uniform standard for defining the requirements for standing, and the majority in *Clapper* admits that the Court has not always required plaintiffs to show that the harm is "literally certain" to occur.[201] The strict standard of *Clapper* should therefore be read narrowly and not apply in all standing cases, given that the Court has allowed more relaxed standards in circumstances that warrant it.[202]

---

[200] *Id.* (citing Babbit v. United Farm Workers Nat'l Union, 442 U.S. 289, 298 (1979), Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U.S. 167, 190 (2000), Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139 (2010), Davis v. Federal Election Commission, 554 U.S. 724, 734 (2008), MedImmune, Inc. v. Genetech, Inc., 549 U.S. 118, 129 (2007), Dep't of Commerce v. U.S. House of Representatives, 525 U.S. 316, 333 (1999), Clinton v. City of New York, 524 U.S. 417, 432 (1998), Pennell v. San Jose, 485 U.S. 1, 8 (1988), Blum v. Yaretsky, 457 U.S. 991, 1001 (1982), Bryant v. Yellen, 447 U.S. 352, 367–368 (1980), *and* Buckley v. Valeo, 424 U.S. 1, 74 (1976)).

[201] *In re Adobe Sys., Inc. Privacy Litig.*, 2014 WL 4379916, *7 (citing *Clapper*, 133 S.Ct. at 1150 n.5).

[202] *See, e.g., Pennell*, 485 U.S. at 8 (the Court uses its "realistic danger" standard to find standing for landlords who

One can view *Clapper*, and similar cases,[203] as controlling precedent in certain cases of increased risk of injury.[204] Alternatively, one can view the standard applied in any particular case as dependent on the facts and context of that case.[205] The standard for standing then depends on the facts and context of each case and courts should have discretion in deciding which standard to apply.[206] This Article now compares the various standards for standing articulated by the Supreme Court in cases prior to *Clapper*. The comparison of these cases is necessary to find a more appropriate standard for the increased risk of identity theft context.

The Supreme Court in *Laidlaw* employed a less demanding standard than the standard employed in *Clapper*.[207] The plaintiff in *Laidlaw* claimed that the continuous dumping of waste in a river would cause the members of the plaintiff's organization to curtail their use of the river.[208] The Court found the plaintiff had standing because the possibility of the injury occurring was not "improbable."[209] *Laidlaw* employed a more relaxed

---

fear their rent will be reduced because of a City Ordinance that would possibly affect them if certain types of tenants seek to rent their units).

[203] *E.g. Whitmore*, 495 U.S. at 157; *Lujan*, 504 U.S. at 563–64.

[204] *Clapper*, 133 S. Ct. at 1147.

[205] *See supra*, Part II, Section A, Subsection 2; *see also Clapper*, 133 S. Ct. at 1153–55.

[206] Local #773 of the Int'l Ass'n of Fighters v. City of Bristol, No. 3:11cv1657 (MPS), 2013 WL 1442453, at *3 (D. Conn. Apr. 9, 2013).

[207] Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U.S. 167 (2000).

[208] *Id.* at 184–85.

[209] *Id.*

standard than *Clapper* because the likelihood of the injury occurring not being "improbable" is surely easier to meet than requiring the injury to be "certainly impending."[210] But it would be difficult to discern the standard from this case because its facts would probably suggest standing even under the certainly impending standard.[211] This is because the plaintiffs provided evidence showing that the affected individuals would respond to the actions of the defendant, and the injury would therefore occur.[212]

The Supreme Court also applied a lower standard for standing in *Monsanto*.[213] The respondents in *Monsanto* feared their crops would be cross pollinated causing their organic crops to be mixed with genetically modified crops.[214] The *Monsanto* Court found that a substantial risk of the injury occurring is enough to grant standing.[215] The Court found the potential for injury to be sufficiently concrete to constitute a substantial risk of injury and held that respondents had standing.[216] This "substantial risk" standard can be viewed as a lower threshold than the "certainly impending" requirement of *Clapper*. This is partially because reaching several of the conclusions required to establish standing in *Monsanto* would require some

---

[210] *See Clapper*, 133 S. Ct. at 1147 (rejecting an "objectively reasonable likelihood" as to light of a standard).
[211] *See id.* at 181–83.
[212] *Id.* (the plaintiffs provided affidavits).
[213] Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139 (2010).
[214] *Id.* at 144–156, 153 n.3.
[215] *Id.* at 153–54.
[216] *Id.* at 155.

speculation.[217] The level of speculation would probably cause the injury in *Monsanto* to fall short of meeting the *Clapper* test for standing.

The Supreme Court in *Davis* used statistical facts to find the appellant had standing to make a claim for his future injury.[218] The appellant challenged a statute that allowed his opponents in a Congressional campaign to receive contributions on terms more favorable than his.[219] The Court allowed standing because most candidates did take advantage of this opportunity, even though the appellant's opponent ultimately did not.[220] The Court employed a standard of the threat being "real, immediate and direct" to find that the appellants' evidence of the likelihood the opponents taking the opportunity was enough to meet the standing requirements.[221] This evidence shows that the event must be foreseeable, and *likely* to happen, as opposed to the "certainly impending" standard that requires evidence that shows the event *will* happen.[222] As the evidence showed, the event that

---

[217] One would have to speculate that the bees would cross pollinate the organic crops with the genetically modified crops and whether the respondents would have to separate the two batches of crops. *Id.* at 153 n.3, 154; *see Lujan*, 504 U.S. at 564 n.2 (the court found the risk of the event happening to be speculative even though the probability of the event happening depends on the respondents' own actions and intent.).

[218] Davis v. Federal Election Comm'n, 554 U.S. 724, 734–35 (2008).

[219] *Id.* at 728, 731–35.

[220] *Id.* (This opportunity was nevertheless available to the appellant's opponent).

[221] *Id.*

[222] *See id.*; *see Clapper*, 133 S. Ct. at 1160 (Breyer, J., Dissenting) (the majority's use of the standard "certainly

the appellant feared did not materialize, even though standing was allowed.[223] Thus, *Davis* definitely uses a lower standard than *Clapper* when finding whether a party has standing.

The Supreme Court in *Yaretsky* used the past occurrence of an event to theorize the likelihood of the event occurring in the future.[224] *Yaretsky* involved nursing home patients facing the threat of being transferred to different facilities, based on the decisions of a committee.[225] The Court found that the threat of the respondents being sent to another health facility with a different level of care was "quite realistic" because a committee had previously made that determination.[226] The Court viewed this evidence as raising the risk of the injury occurring over the level of "imaginary or speculative."[227] This "quite realistic" standard does not seem as restrictive as *Clapper*'s "certainly impending" standard. In fact, it relies on a degree of speculation as to whether the nursing home would repeat its determination of the respondent's level of care in the future.[228] *Yaretsky* utilizes a slightly lower standard than that of *Clapper*.

Overall, there are several Supreme Court cases that have applied less strict standards than the certainly impending standard in *Clapper* to find that a party to a case has standing. But there are several

---

impending" requires evidence that the event *will* happen.) (emphasis added).

[223] *Davis*, 554 U.S. at 734.

[224] Blum v. Yaretsky, 457 U.S. 991, 1000–1001 (1982).

[225] *Id.* at 994–95.

[226] *Id.* at 1000–1001.

[227] *Id.* (citing O'Shea v. Littleton, 414 U.S. 488, 496 (1982) ("past wrongs are evidence bearing on whether there is a real and immediate threat of repeated injury")).

[228] *See id.*

other highly cited cases that have found a party does not have standing.[229] These cases will be considered to show that they generally use more lenient standards than that in *Clapper*, and the failure of standing in those cases was based on the facts before the Court.

The Supreme Court did not allow standing on a set of attenuated facts in *Whitmore*.[230] This case involved a death row inmate, who had exhausted all of his appeals, hoping for a favorable decision in another death row inmate's case.[231] For this inmate's injury to occur, there would need to be habeas corpus relief in the future granting him a new trial, he would have to be convicted again and sentenced to death again, and on review of the sentence, the Court would have to compare his sentence to that of the other inmate.[232] The Court found the injury too speculative to support standing.[233] The Court further found that "[a]llegations of possible future injury do not satisfy the requirements of Art. III" and "[a] threatened injury must be 'certainly impending' to constitute injury in fact,"[234] which is in line with the strict holding of *Clapper*.[235] But the Court in

---

[229] *See, e.g.*, *Whitmore*, 495 U.S. 149 *and Lujan*, 504 U.S. 555.
[230] Whitmore v. Arkansas, 495 U.S. 149, 157 (1990).
[231] Id. at 151–154, 156–157
[232] *Id.*
[233] *Id*. (the court especially found problematic the first step of the inmate eventually securing habeas relief and receiving a new trial).
[234] *Id.* at 158 (citing Babbitt v. Farm Workers, 442 U.S. 289, 298 (1979)).
[235] *Clapper*, 133 S. Ct. at 1147–1148 (*Clapper* expressly incorporates the "certainly impending" standard from *Whitmore*).

Whitmore acknowledge certain situations where an attenuated injury would be sufficient to support standing.[236] The conclusion from *Whitmore* should be that attenuated injuries can sustain standing only if it is possible to be proven at trial that the risk of those injuries is immediate.

The Supreme Court in *Lujan* perhaps used a very strict standard in denying standing.[237] In *Lujan*, several organizations challenged a statute, which was re-interpreted in a way that they believed could cause the destruction of natural ecosystems.[238] The injury claimed was that the members of these organization would not be able to visit and see these ecosystems in the future.[239] But this claim of injury was insufficient because not only was the alleged damage to the ecosystem speculative, but the person visiting the site at some unknown time in the future was also speculative.[240] Thus, the Court did not allow standing based on this theory because of the speculation required for the events.[241] This case raised the standard of what is speculative because although the plaintiff had control over the injury occurring, the plaintiff did

---

[236] *Whitmore*, 495 U.S. 149, 158–60 (citing U.S. v. SCRAP, 412 U.S. 669, 693 (1973)) (*Whitmore* distinguishes *SCRAP* by stating the injuries in *SCRAP* could have been proven at trial to be at risk of happening immediately, while the injuries in *Whitmore*, the court determined themselves, could not be proven at trial to have a risk of happening immediately.).
[237] Lujan v. Defenders of Wildlife, 504 U.S. 555, 563–64 (1992).
[238] *Id.* at 558–59.
[239] *Id.* at 562–64; *see also id.* (citing Sierra Club v. Morton, 405 U.S. 727, 734 (1972) ("the desire to use or observe an animal species, even for purely esthetic purposes, is undeniably a cognizable interest for purpose of standing.")).
[240] *Id.* at 563–64.
[241] *Id.*

not have a plan to complete the events which would cause the injury to materialize.[242]

The different standards were applied with different sets of facts and in different contexts. Therefore, contrary to post-*Clapper* increased risk of identity theft cases that denied standing, the "certainly impending" standard is not the only standard available for establishing standing. The determination of what standard should be applied should be flexible and should depend on the facts and contexts of the particular case.

C. *THE APPROPRIATE STANDARD FOR INCREASED RISK OF IDENTITY THEFT*

1. Explanation of the "Highly Likely" Standard

A more suitable standard for increased risk of identity theft cases would be a combination of the standards from *Laidaw*[243] and *Davis*[244] and possibly the standard presented in *Yaretsky*.[245] *Laidlaw* used a standard of whether the injury occurring was improbable, to find that the possibility of certain people not using a lake after a company's dumping of toxic material was not too speculative.[246] The Court in *Davis* used the standard of whether the threat of injury was "real, immediate and direct" to find that the plaintiff's opponents using the benefit of a statute affecting campaign

---

[242] *See id.*
[243] *Laidlaw*, 528 U.S. at 184–85.
[244] *Davis*, 554 U.S. at 734–35.
[245] *Yaretsky*, 457 U.S. at 1000–01.
[246] *Laidlaw*, 528 U.S. at 184–85.

contributions was not too speculative in the face of evidence that the opponents usually do take advantage of the benefit.[247] These cases are more in line with the identity theft cases because they both involve steps that require very little speculation as opposed to the heavy speculation required in *Clapper*. In *Davis*, there was statistical facts showing that the event was more likely to happen,[248] similar to data breach cases where statistics show that a victim of a data breach is more likely to suffer from identity theft in the future.[249] *Laidlaw* similarly is more comparable because in *Laidlaw* there were affidavits from individuals that they were likely to avoid the lake if the dumping of the toxic material continued.[250] Similarly in the identity theft cases, there is usually evidence that somebody has the information,[251] and from looking at the environment of identity theft laws, one conclusion that can be drawn is that once somebody has the information, there is little speculation required to conclude that they would use the information.[252]

Furthermore, adding *Yaretsky* into the equation, one conclusion that could be drawn from evidence of an attempted incident of identity theft using the stolen data, is that there may be another

---

[247] *Davis*, 554 U.S. at 734–35.
[248] *Id.*
[249] Carrns, *supra* note 6.
[250] *Laidlaw*, 528 U.S. at 184–85.
[251] *See Krottner*, 628 F.3d at 1140–41 (the laptop was stolen, and somebody actually used the plaintiff's information); *see Pisciotta*, 499 F.3d at 632 (the "intrusion was sophisticated, intentional and malicious); *see Reilly*, *supra* notes 112–123 (the breach was likely intentional, so it is highly likely somebody has the information).
[252] *See* Carrns, *supra* note 6.

attempt in the future and therefore the future risk of identity theft is less speculative. This is because the Court in *Yaretsky* reasoned that if an event happened in the past,[253] it is more likely to happen in the future.[254] In relying on *Yaretsky*, the risk of the event is more than "imaginary or speculative."[255] One of the few courts that might disagree with the holding from *Yaretsky* is the Sixth Circuit in *Lambert v. Hartman*.[256] However, all the Sixth Circuit does in *Lambert* is give a conclusion on why standing should not be allowed, without providing an analysis.[257] The Sixth Circuit *Lambert* was wrong in its conclusion on that issue, and the court in *Krottner* subtly suggests that *Lambert* is wrong.[258] *Lambert* is more similar to *Yaretsky* because it involves an attempt to use the plaintiff's stolen information, so it should have allowed standing on the increased risk of identity theft issue.

The facts in the increased risk of identity theft cases are more similar to those constitutional standing cases where standing was allowed.[259] The

---

[253] *Yaretsky*, 457 U.S. at 1000–1001 (in *Yaretsky*, it was the context of a nursing home previously making a certain determination, so they were likely to make that determination in the future).
[254] *See id.*
[255] *Id.*
[256] *See* Lambert v. Hartman, 517 F.3d 433, 438 (6th Cir. 2008) (the court stated in dicta that "the risk the information would be used by somebody to commit future acts of identity theft against the plaintiff is somewhat 'hypothetical' and 'conjectural.'").
[257] *Id.*
[258] *See Krottner*, 628 F.3d at 1143 (acknowledging that Lambert does not give an analysis and stating that they will come up with a different conclusion on their facts).
[259] *See Laidlaw*, 528 U.S. at 190, *Monsanto*, 561 U.S. at 139, *Davis*, 554 U.S. at 734, *and Yaretsky*, 457 U.S. at 1001.

standards from those cases are therefore more suitable to govern the identity theft cases. Considering all the facts and the analysis above, the most appropriate is requiring the injury to be highly likely but not certain to occur. This standard remains higher than there being a mere possibility of the injury occurring, so there is a firm threshold, but it keeps it at an accessible level for most plaintiffs who have a genuine risk of suffering from identity theft in the future.

In proving that the possibility of suffering from identity theft is highly likely, the plaintiff must first show that the only steps required for the injury to occur are for a third party to obtain the information and for that third party to use the information in a malicious way. The plaintiff must then present evidence to show that it is highly likely that the third party has the information and that the third party would use the information, which is often the case when the third party has the information.[260] Showing that a third party has the information can be done with evidence that the theft of the information or the breach of the system the information was obtained in was intentional.[261] Some other evidence to show an intentional breach includes stolen laptops in certain situations.[262] Some supplemental evidence may include the

[260] *See* Carrns *supra*, note 6.

[261] *See Pisciotta*, 499 F.3d at 632; *see Reilly*, *supra* notes 112–123.

[262] *See Krottner*, 628 F.3d at 1140; Resnick v. AvMed, Inc., 693 F.3d 1317, 1322 (11th Cir. 2012); Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 910 (N.D. Cal. 2009) (the laptops in all three cases were stolen from corporate offices. Additionally, in two of the cases, there were uses, or attempted uses of the information and in the last case, the information was visible on the laptop during the theft.).

plaintiff suffering from an attempted incident of identity theft, which would show that somebody likely had the information.[263]

2. Application of the "Highly Likely" Standard

In applying this new standard to the identity theft cases in the Circuit split, this new standard of the injury being highly likely will create a logical solution. When applying the standard to the facts in *Krottner*, it is highly likely that the injury would occur in the future because of the limited number of logical steps required to reach that conclusion.[264] The probability of the injury occurring was less than speculative because the plaintiffs presented evidence of an intentional laptop theft[265] together with evidence of a failed attempt of identity theft.[266] The facts in *Pisciotta* would also meet the highly likely standard because there were few logical steps required to conclude that the injury would occur.[267] The probability of injury occurring was less than speculative because the plaintiff presented evidence that the theft was intentional, sophisticated and malicious.[268] Finally, the facts in *Reilly* would also meet the highly likely standard, although the determination would be a little more difficult in this case; there were few steps required for the injury to

---

[263] *See Krottner*, 628 F.3d at 1141; Lambert v. Hartman, 517 F.3d 433, 436–37 (6th Cir. 2008); Resnick v. AvMed, Inc., 693 F.3d 1317, 1322 (11th Cir. 2012).
[264] *See supra*, Part II, Section B, Subsection 1.
[265] *See Krottner*, 628 F.3d at 1140.
[266] *See id.* at 1141.
[267] *See supra*, Part II, Section B, Subsection 1.
[268] *Pisciotta*, 499 F.3d at 632.

occur,[269] and the probability of the injury occurring was less than speculative because the facts of the case indicated that the breach was likely to be intentional.[270] Overall, this new test could be applied perfectly to the cases in the Circuit split to not only resolve the Circuit split, but also to allow plaintiffs in those cases to have standing and proceed with their respective cases.

There are other examples of cases in which the Court did not find standing, but where it would have under this new and refashioned standard.[271] For example, the court *in re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation* did not find standing because the injury alleged by the plaintiff was too attenuated and speculative.[272] But in *SAIC*, the plaintiffs alleged that some of the individuals involved suffered from identity theft after the incident in question.[273] Therefore, under the highly likely standard, there would have been sufficient evidence presented to support standing.[274]

This new test will not allow standing in all instances. The fact that this new standard will not allow standing where the plaintiff is only alleging a mere possibility that the identity theft would occur is instrumental in denying standing to the plaintiffs

---

[269] *See supra*, Part II, Section B, Subsection 1.
[270] *See Reilly*, *supra* notes 117–121 (this is what makes the analysis in *Reilly* more difficult because *Reilly*, unlike *Krottner* and *Pisciotta*, did not explicitly state that the theft was intentional.).
[271] *See in re* Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation, No. 12-347 (JEB), 2014 WL 1858458 (D.D.C. May 9, 2014).
[272] *Id.* at *9.
[273] Id. at *1–2.
[274] *Yaretsky*, 457 U.S. at 1000–1001.

who are attempting to bring a case with little or no evidence that the identity theft would in fact occur.[275] An example of this is when a plaintiff information is only lost, and there is no evidence of the intentional act of a third party.[276] These types of cases would require more speculation than the average data breach cases because one would have to speculate that the information was stolen, that somebody is in possession of it and that the information will be misused.[277] The highly likely standard imposes a minimum threshold for standing to be established, and if one cannot show that somebody else is likely to have the information, then they will fail under the highly likely standard.

There is another set of cases where a claim for standing under an increased risk of identity theft would fail under the highly likely standard. These are cases where the medium that contains the information has intrinsic value and it is not readily apparent that the theft was for anything other than the medium's value. An example might be the random theft of a laptop, containing personal information, from vehicle.[278] The theft by itself

---

[275] *See supra,* Part II, Section B, Subsection 1 (the highly likely standard is higher than the injury being only a mere possibility.).

[276] *E.g.* Giordano v. Wachovia Securities, LLC, Civil No. 06-476 (JBS), 2006 WL 2177036, at *1 (D.N.J. July, 31, 2006) (where the plaintiff's personal information was on documents lost in the mail); Hammond v. The Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307 (S.D.N.Y. June 25, 2010) (where tapes containing the plaintiff's personal information were lost while in transit).

[277] Giordano v. Wachovia Securities, LLC, Civil No. 06-476 (JBS), 2006 WL 2177036, at *5 (D.N.J. July, 31, 2006).

[278] *E.g.* Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 456–457 (D.N.J. 2013); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., No. 12-347 (JEB), 2014 WL

shows nothing more than a random criminal act, and one would have to speculate whether the thief accessed the laptop and realized the value of the information on that laptop.[279]

Another question arises when the primary evidence used to show an increased risk of identity theft after a data breach is an actual incident of identity theft or attempted identity theft. The question that arises is whether causation is met.[280] This is based on *post hoc ergo propter hoc* ("after this, therefore because of this"), which is the belief that just because one event occurred after the other, does not mean the first caused the second.[281] Courts have used this reasoning to find that causation is not met where a plaintiff is arguing that it was the data breach that caused the actual incident of identity theft.[282] But this reasoning is incorrect because the plaintiff does not need to show that the data breach was absolutely the cause of the identity theft, only that it is reasonably likely that the data breach caused the identity theft.[283] There are some instances in which it is easy to prove the information used in the identity theft was from the data breach, such as in *Lambert v. Hartman*, where

---

1858458 (D.D.C. May 9, 2014) (where several electronics, including data tapes containing personal information, were stolen from a vehicle).

[279] *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., No. 12-347 (JEB), 2014 WL 1858458, at *6 (D.D.C. May 9, 2014).

[280] Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906, at *5 (D. Ariz. Sept. 6, 2005).

[281] *Id.* at *7.

[282] *See e.g. id.* (but this still remains a gray area in the law since only a few courts have taken on this issue.).

[283] *See id.* at *5.

the data released and the information used in the incident of identity theft both had the same incorrect driver's license number.[284] The typical identity theft case may not be that easy, but should still allow standing if: 1) the same type of information used in the identity theft incident was a part of the data breach, 2) the identity theft incident occurred shortly after the data breach and 3) there are no other clear sources of leaked information the identity thief could have obtained the information from.[285]

The consideration of whether the actual incident of identity theft can support the increased risk should be based on the three requirements above. The first requirement being the same type of information would narrow the source such as if the only information leaked was a person's name and their health information and the identity thief used their credit card information, then that would not create a causal relationship. With respect to the second requirement, an identity thief will typically uses the information as soon as he or she is able because such information declines in value with time;[286] an identity theft incident occurring shortly

---

[284] Lambert v. Hartman, 517 F.3d 433, 435–36 (6th Cir. 2008).

[285] *See* Stollenwerk v. Tri-West Health Care Alliance, 254 Fed. Appx. 664, 667–68 (9th Cir. 2007).

[286] The commercial value of stolen information declines over time. Tom Zeller, Jr., *Black Market in Stolen Credit Card Data Thrives on Internet*, N.Y. TIMES, June 21, 2005, http://www.nytimes.com/2005/06/21/technology/21data.html; *See*, *also*, Fu v. Wells Fargo Home Mortg., No. 2:13-cv-01271-AKK, 2014 WL 4681543, *2, *4–5 (N.D. Ala. Sept. 12, 2014) (slip copy) (not finding causation where the actual incident of identity theft occurred over a year after defendant mishandled plaintiff's information.)

after a data breach would create a stronger causal relationship. The final requirement, there being no other clear source of the data being leaked, is merely a process of elimination. If there have not been any other data breaches within the time period, the person has been cautious on the internet and generally cautious with their identity, then the data breach in question is the only clear cause of the identity theft. Of course there are other possible ways an identity thief could obtain the information,[287] but there is a small chance of those occurring, and the most likely cause is the data breach. This third requirement alone cannot establish causation, but together with other elements such as the requirements above, can make a strong case for causation and therefore allow the evidence of the identity theft incident to be used in establishing an increased risk of identity theft.

Overall, the highly likely standard would provide guidance to the great majority of cases and will produce a fair and logical result, allowing standing where the plaintiffs have a genuine fear of suffering from identity theft in the future as opposed to situations where the plaintiff's fears are unfounded.

III. IMPLICATIONS OF THE NEW STANDARD

Although many courts disagree that a more relaxed standard should be used in increased risk of identity theft cases, to allow this standard would be a disservice to the original purposes the

[287] Such as the information getting lost in the mail. *See* Giordano v. Wachovia Securities, LLC, Civil No. 06-476 (JBS), 2006 WL 2177036, at *1 (D.N.J. July, 31, 2006)

justiciability requirement of the Constitution.[288] There are two ways this relaxed standard can be justified, the first being that increased risk of identity theft cases are analogous to contexts where courts agree should have a lower standard and the second being that the remedies could be adjusted to be more appropriate for these types of cases.

Increased risk of identity theft cases may be analogized to other future injury contexts where a lower standing has been allowed. Some courts have argued that data breaches are different from the defective medical devices and toxic tort cases where standing has been allowed because in those cases, there is a present injury.[289] But an argument can be made that there is in fact an injury in cases of data breaches since the individual is losing control over their information.[290] Although the present injury is not as severe in the increased risk of identity theft cases, there is arguably an injury nonetheless.

The critics of the lenient standard may argue that it would it would increase litigation since more plaintiffs could sue.[291] The answer to this is to limit the remedies available in the average case. One of the most logical remedies is for the defendant to

---

[288] For further analysis about justiciability requirement, *see* Galbraith, *supra* note 49, 1386.

[289] *Reilly*, 664 F.3d at 45 (citing Sutton v. St. Jude Medical S.C., Inc., 419 F.3d 568 (6th Cir. 2005).

[290] Lexi Rubow, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKELEY TECH. L.J. 1007, 1012–13 (2014).

[291] Patricia Cave, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier From Federal Courts in Data Security Breach Suits*, 62 CATH. U.L. REV. 765, 786 (2013).

pay for the plaintiff's credit monitoring costs. Credit monitoring is important for anybody considering to protect themselves from identity theft, and it especially becomes invaluable when somebody is at a much higher risk of suffering from such identity theft. One example is LifeLock, which monitors your personally identifiable information, scans for threats to your personally identifiable information, alerts you when they suspect a threat, guarantees $1 million of protection, and tracks your credit score.[292] Furthermore, case law has stated that credit monitoring is an appropriate remedy in the case of identity theft.[293] Overall, providing credit monitoring as damages would provide a means in which the plaintiff could protect their credit, but as explained above, will not be overly burdensome on the defendant.

IV. CONCLUSION

This Article proposes a highly likely standard to be applied to cases of an increased risk of identity theft as opposed to the stricter "certainly impending" standard used in *Clapper*. This would produce a more just result since the context that *Clapper* was decided in is fundamentally different from the increased risk of identity theft context. Not only is there a stark contrast between the data breach and the national security and constitutional law contexts, the facts in *Clapper* made the injury alleged there far less impending than the typical identity theft case. So the new standard of highly

[292] LIFELOCK, 5 POINTS OF PROTECTION, http://www.lifelock.com/how-it-works/ (last visited Jan. 8, 2015).
[293] Lambert v. Hartman, 517 F.3dd 443, 438 (6th Cir. 2008).

likely would be more appropriate since it is derived from a line of Supreme Court cases whose facts are more similar to the typical increased risk of identity theft case than is *Clapper* and whose standard is far less strict than that of *Clapper*. It would allow for a remedy for the victims of a data breach without them having to wait until they actually suffer from identity theft. Further, because there are certain situations proposed in this standard where standing should not be allowed, this new standard will not open the floodgates of litigation after a data breach. As a remedy, credit monitoring costs would be the most appropriate in the majority of cases, so as to justify lowering the standard for these types of cases. In conclusion, data breaches and identity theft will not stop in the near future, to the contrary, they will most likely increase, so lawmakers and the judiciary should contemplate a final solution which is fair to all parties.