TOURO UNIVERSITY
JACOB D. FUCHSBERG LAW CENTER
Where Knowledge and Values Meet

Touro Law Review

Volume 36 | Number 4 Article 18

2021

No Standing and No Recourse: The Threat to Employee Data Under Current U.S. Cybersecurity Regulation

Georgia D. Reid
Touro Law Center

NO STANDING AND NO RECOURSE: THE THREAT TO EMPLOYEE DATA UNDER CURRENT U.S. CYBERSECURITY REGULATION

*Georgia D. Reid**

I. INTRODUCTION

The computer and digital revolution in the mid-twentieth century rapidly evolved into today's information age. Unlimited data, media, and information are at our fingertips, and our daily lives depend on smart devices and lightning-fast communication. The amount of data on the internet is growing exponentially, which inevitably creates a larger attack surface for cybercriminals and hackers.[1] According to the FBI's Internet Crime Report, the cost of cybercrimes reached $2.7 billion in 2018.[2] We hear about cybercrime in the news when major data breaches occur, resulting in class action lawsuits involving consumers.[3] For example, in 2013, two retail gi-

---

* Touro College Jacob D. Fuchsberg Law Center, J.D. Candidate 2021; Hunter College, M.A. in English Education, 2007; University of Massachusetts, Amherst, B.A. in English, 2003. I would like to give a special thanks to my family for their unconditional love and support in everything that I do. Next, thank you to my friend, colleague, and notes editor, Alessandra Albano, for her continued guidance throughout the writing and editing process. I give many thanks to my faculty advisor, Professor Rena Seplowitz, for encouraging me to challenge myself in law school and to apply to the Law Review. Thank you to the entire staff and editorial board of the Touro Law Review for being so supportive and helpful during the process of getting this Note ready for publication. Professor Meredith Miller and Professor Michelle Zakarin also helped me form the idea for this Note and I thank them as well.

[1] Jeff Schultz, *How Much Data is Created on the Internet Each Day?* MICRO FOCUS BLOG (August 6, 2019), blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day. ("In 2014, there were 2.4 billion internet users. That number grew to 3.4 billion by 2016, and in 2017, 300 million internet users were added. As of June 2019, there are now over 4.4 billion internet users.").

[2] *Internet Crime Report 2019*, FBI, www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited July 18, 2020).

[3] *See* cases cited *infra* note 4.

ants were attacked.[4] Hackers installed malware in Neiman Marcus' systems which "siphoned customer card information during transactions."[5] A similar attack occurred at Target, compromising the information of 110 million customers.[6] The cost to the companies not only to repair their systems, but also to settle with consumers, was massive.[7] Target avoided going to court, but paid an $18.5 million multistate settlement, the largest ever for a data breach.[8]

Shopping is something people do for pleasure and even for survival.[9] Large stores like Target and Neiman Marcus became prime targets for hackers because of their large attack surface of credit card numbers.[10] Personal identification information (PII), stored by

---

[4] *See, e.g.,* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 690 (7th Cir. 2015); *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014).

[5] Kelly Jackson Higgins, *1.1 Million Payment Cards Exposed in Neiman Marcus Data Breach*, DARK READING, (Jan. 23, 2014, 7:25 PM), www.darkreading.com/attacks-breaches/11-million-payment-cards-exposed-in-neiman-marcus-data-breach/d/d-id/1141212. This means that hackers stole credit card information when customers used these cards at checkout in the brick-and-mortar stores. *Id.*

[6] Michael Kasner, *Anatomy of the Target data breach: Missed opportunities and lessons learned*, (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned.

[7] *See* McCoy *infra* note 8.

[8] Kevin McCoy, *Target to pay $18.5M for 2013 data breach that affected 41 million consumers*, USA TODAY, (May 23, 2017, 6:42 PM), www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932.

[9] Katie Evans, *More Than One Third of Consumers Shop Online Weekly since Coronavirus Hit*, DIGITAL COMMERCE 360, (Oct. 1, 2020), https://www.digitalcommerce360.com/2020/10/01/more-than-one-third-of-consumers-shop-online-weekly-since-coronavirus-hit/ ("36% of respondents shop online weekly, up from 28% pre-Covid-19, according to a July survey of 5,000 consumers in North American and Europe from Selligent, which provides omnichannel marketing services to companies, including retailers and brands."); *Neiman Marcus Emerges from Bankruptcy*, September 20, 2020, CNBC, www.cnbc.com/2020/09/25/neiman-marcus-emerges-from-bankruptcy.html. Ironically, Neiman Marcus filed for Chapter 11 bankruptcy protection, emerging from one of the highest-profile retail collapses during the Covid-19 pandemic.

[10] Brian Krebs, *Target Investigating Data Breach*, KREBS ON SECURITY, (Dec. 13, 2013), krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/ ("Target released a statement this morning confirming a breach, saying that40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. . . . In 2007, retailer TJX announced that its systems had been breached by hackers. . . . [who]made off with data from more than 45 million customer credit and debit cards.").

human resource departments, is valuable to hackers as well.[11] An attack might involve ransomware, holding critical hardware hostage until a large sum of money is paid or other data is handed over.[12] Cybercrime can result in identity theft, which occurs when hackers steal personal information from a database to later abuse or sell to the highest bidder.[13] According to the FBI, identity theft is increasingly being facilitated on the internet.[14]

If someone's identity, credit card information, or other personal data is compromised, a victim can either sue the hackers, or sue the company that was hacked. It is nearly impossible to prosecute the criminals themselves because they generally reside overseas.[15] In the cases involving Nieman Marcus and Target, the stores themselves were held responsible.[16] In the 2015 case *AFGE v. OPM* (In re United States OPM Data Sec. Breach Litig.) ("OPM"),[17] hackers may have stolen the names, Social Security numbers, addresses and other information of federal workers.[18]

---

[11] Aliah D. Wright, *Federal Government Hacked: Lessons for HR*, (June 12, 2015), www.shrm.org/resourcesandtools/hr-topics/technology/pages/what-are-the-lessons-for-hr-in-government-hacking.aspx ("Employee and health care data (as opposed to cardholder data) are increasingly targeted for theft . . . [w]hat could hackers want with this information? To commit identity theft? Fraud? Blackmail? Discover who has more sensitive data than others? All of the above, experts say.").

[12] Josh Fruhlinger, *Ransomware explained: What It Is and How to Remove It*, CSO (June 20, 2020 3:00 AM), www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html ("Ransomware is a form of *malware* that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.").

[13] *See* FBI *infra* note 14.

[14] *What We Investigate: Cyber Crime*, FBI, www.fbi.gov/investigate/cyber (last visited May 28, 2020). The FBI is the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists. *See id.* The nation's critical infrastructure, including both private and public sector networks, are targeted by adversaries. *Id.* American companies are targeted for trade secrets and other sensitive corporate data and universities for their cutting-edge research and development. Citizens are targeted by fraudsters and identity thieves, and children are targeted by online predators. *See id.*

[15] Toshendra Sharma, *The World's Top Ten Cybercrime Hotspots,* (Nov. 28, 2019), GLOBAL TECH COUNCIL, www.globaltechcouncil.org/blockchain/worlds-top-10-cyber-crime-hotspots/. China, Brazil, Russia, Poland, Iran, India, Nigeria, Vietnam, and Germany are currently the world's international cybercrime hotspots. *See id.*

[16] *See* cases cited *infra* note 19.

[17] 928 F.3d 42 (D.C. Cir. 2019).

[18] *Id.* at 49.

There are many recent cases about consumer data stolen from retail establishments, as well as some involving healthcare facilities, technology platforms, and financial institutions.[19] Cybercriminals (hackers) steal data, but what subsequently happens to the data is difficult to determine because cybercriminals do not tend to use the data themselves; they typically post stolen data on forums on the dark web where they can be sold for profit.[20] Federal circuits are split as to whether plaintiffs even have standing to sue in data breach cases because the risk of harm to the plaintiff is remote and hard to trace.[21] The First, Second, Third, and Fourth Circuits take a strict approach, holding that the injury to the plaintiffs is too speculative to confer standing.[22] The Sixth, Seventh, Ninth, Eleventh, and D.C. Circuits found that a mere future risk of identity theft does justify standing.[23]

When cybercriminals attack a business, that business is the victim of a crime and should be treated as such. As a victim of this attack, the company must also prepare to be sued by customers or employees, which creates a "victim defendant" dichotomy.[24] The challenge is how to judge a company's compliance when the only legal standard companies need to adhere to is "reasonably prudent" cy-

---

[19] *Compare*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015), *with* Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524 (D. Md. 2016), *and* In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295 (N.D. Ga. 2019), *and* Collins v. Athens Orthopedic Clinic, P.A., 837 S.E.2d 310 (Ga. 2019).

[20] *After the Breach, What Happens to Your Data?* BLACKFOG (July 9, 2019), www.blackfog.com/after-the-data-breach-what-happens-to-your-data ("The value data of data changes and is affected by many factors including supply and demand . . . .").

[21] *See* cases *infra* note 22.

[22] *See, e.g.,* Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017) (holding that plaintiff's allegations in the complaint did not suffice to establish Article III standing); Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) ("To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'"); Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017) ("Our sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft.").

[23] *See, e.g.,* Resnick v. Avmed, Inc., 693 F.3d 1317, 1323 (11th Cir. 2012).

[24] Adam Brouillet, *The Legal Implications of Cybersecurity When Collecting Personal Information*, (Aug. 14, 2018), FINANCIAL POISE, www.financialpoise.com/when-collecting-personal-information/ (explaining that due to the "victim defendant" dichotomy, businesses should purchase cybersecurity insurance).

bersecurity measures.[25] Absent a law that clarifies the duty of employers to protect the PII of employees, this Note argues that a company's cybersecurity measures will continue to be judged on a case by case basis. Additionally, cybercriminals are notoriously "one step ahead" of technology and will often outsmart the most prudent of cybersecurity measures.[26]

Part II of this Note provides an overview of data privacy and cybersecurity laws, as well as current best practices for companies. Part III summarizes what plaintiffs must establish for standing to sue by briefly discussing the Supreme Court cases *Ashcroft v. Iqbal,*[27] *Bell Atlantic Corp. v. Twombly*,[28] and *Clapper v. Amnesty International*.[29] Part IV analyzes the circuit split and argues that the First, Second, Third, and Fourth Circuits are correct in taking a strict approach because the fear of a future harm is too remote to establish standing in data breach cases. Part V examines cases involving the theft of employee data, including *AFGE v. OPM (In re United States OPM Data Security Breach Litigation),*[30] a 2019 United States Court of Appeals for the District of Columbia Circuit case.[31] Part VI looks at the legal duties owed to employees by employers, exposing a lack of protection for employee data. This section also compares current United States law to the General Data Protection Regulation ("GDPR") in the European Union ("EU"). Part VII concludes that, due to a lack of incentive to invest in adequate cybersecurity practices and the lack of standing for employees to sue, a change in policy is

---

[25] *Id.*

[26] *Cybersecurity – The Never Ending Cycle,* SECURE 360(July 19, 2016), secure360.org/2015/10/cybersecurity-the-never-ending-cycle ("Cybersecurity seems to be a vicious, never-ending cycle of the 'good guys' stepping up their security and training to prevent attacks, only to be followed by the 'bad guys' discovering new methods to infiltrate systems.").

[27] 556 U.S. 662 (2009) (holding that detainee's complaint failed to plead sufficient facts to state claim for purposeful and unlawful discrimination).

[28] 550 U.S. 544 (2007) (holding that dismissal for failure to state a claim upon which relief may be granted does not require appearance, beyond a doubt, that plaintiff can prove no set of facts in support of claim that would entitle him to relief).

[29] 568 U.S. 398 (2013).

[30] 928 F.3d 42 (D.C. Cir. 2019).

[31] *Id.* This case was decided in 2019 and involved federal employees whose personal information was stolen via a cyberattack from their human resources departments.

needed to address the absence of legal recourse for employees whose PII has been compromised.

II. OVERVIEW OF CURRENT DATA PRIVACY AND CYBERSECURITY LAWS IN THE UNITED STATES

Relative to the history of American law, the area of cybersecurity law is in its infancy. The 1988 Children's Online Privacy Protection Act ("COPPA") was the first federal act to govern online activities.[32] Internet privacy is not a human right in the United States.[33] While other industrialized nations, such as Canada and the EU, treat the private data of a citizen as belonging to the person the information describes, the United States is more deferential to business and law enforcement.[34]

American law currently requires companies to notify customers and employees if there is a data breach.[35] However, no federal data privacy framework exists which private organizations are mandated to follow, nor is there any federal data breach notification framework.[36] Signed into law on December 18, 2015, The Cybersecurity Information Sharing Act of 2015 ("CISA") calls on public and

---

[32] 15 U.S.C.A. § 6502. COPPA regulates unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet.

[33] THERESA M. PAYTON & THEODORE CLAYPOOLE, PRIVACY IN THE AGE OF BIG DATA 248 (Rowman & Littlefield 1st ed. 2014) ("While the U.S. Constitution specifically protects a number of liberties that can only reach their full fruition though privacy, the document never mentions privacy as a fundamental right or even an important concept.").

[34] *Id.* at 248 ("Under the laws of these countries, the ability to say what happens to information about you is a human right, and neither government nor business can take and use this information about you without your permission."). *See also* Jeff Kosseff, *Cybersecurity of the Person*, 17 FIRST AMEND. L. REV. 343, 343 (2018).

[35] Kosseff, *supra* note 34, at 343 ("U.S. cybersecurity law is largely an outgrowth of … concerns over identity theft and financial fraud. Cybersecurity laws focus on protecting identifiers such as driver's licenses and social security numbers, and financial data such as credit card numbers. Federal and state laws require companies to protect this data and notify individuals when it is breached and impose civil and criminal liability on hackers who steal or damage this data.").

[36] *Complete Guide to Privacy Laws in the U.S.*, VARONIS, www.varonis.com/blog/us-privacy-laws (last viewed May 25, 2020) ("[T]here isn't a central federal level privacy law, like the EU's GDPR. There are instead several vertically-focused federal privacy laws, as well as a new generation of consumer-oriented privacy laws coming from the states.").

private entities to share information relevant to cybersecurity.[37] Forty-eight states and the District of Columbia now have individual data-breach notification systems in place.[38] The responsibility to develop controls and policies therefore lies with individual, private organizations. Companies and employers must meet general standards, any applicable current state laws, and any other federal regulations that are in place, if they even know where to look.[39] In thirty-eight of the states with breach notification laws, companies can avoid notification obligations if they determine that the breach did not create a risk of harm for individuals whose PII was exposed, which can sometimes be determined by an expensive forensic investigation.[40]

To date, three federal acts regulate industry specific PII, but no act regulates how employees should handle employee PII.[41] Federal regulations are currently in place to protect customers of financial institutions over which the Federal Trade Commission ("FTC") has jurisdiction.[42] In 2002, Congress passed The Standards for Safeguarding Customer Information Act ("SSCIA").[43] Additionally, the

---

[37] CYBERSECURITY INFORMATION SHARING ACT, 6 U.S.C. § 1501 (2015). This is not a mandate and businesses have the option of participating. *See id.*

[38] *Security Breach Notification Laws*, NCSL, (Apr. 12, 2017), www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[39] Hardeep Singh, *A Glance at the United States Security Laws*, APPKNOX, (Jan. 7, 2016) www.appknox.com/blog/united-states-cyber-security-laws. Bruce Schneier, founder of Cupertino's Counterpane Internet Security, stated that "companies will not make sufficient investments in cybersecurity unless government forces them to do so." *Id.* He also states that "successful cyber-attacks on government systems still occur despite government efforts." *Id.*

[40] *See* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1010 (2018).

[41] *See* Singh, *supra* note 39. The Standards for Safeguarding Customer Information Act, HIPAA, and The Homeland Security Act of 2002 are the three Federal Acts that involve cybersecurity. *Id.* These laws "mandate that healthcare organizations, financial institutions, and federal agencies should protect their systems and information. However, these rules are not foolproof in securing the data and require only a 'reasonable' level of security. *Id.*

[42] *See* Standard for Safeguarding Customer Information, 84 Fed. Reg. 131518 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. 314).

[43] *Id.*("The proposal contains five main modifications to the existing Rule. First, it adds provisions designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program. Second, it adds provisions designed to improve the accountability of financial institutions' information security programs. Third, it exempts small businesses from certain requirements. Fourth, it expands the definition of 'finan-

Health Insurance Portability and Accountability Act ("HIPAA") of 1996 protects PII relating to healthcare data.[44] Finally, the Homeland Security Act ("HSA") of 2002 defines cybersecurity threat terms and governmental defense measures for critical infrastructure.[45]

The SSCIA regulates the handling of customer information by all financial institutions over which the FTC has jurisdiction.[46] This act states that these institutions must "develop, implement, and maintain a comprehensive information security program" that is "appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."[47] The objectives of the SSCIA are to (1) ensure the security and confidentiality of customer information, (2) protect against any anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to, or use of such, information that could result in substantial harm or inconvenience to any customer.[48]

HIPAA contains security standards for the healthcare industry, which includes electronically stored data.[49] Prior to HIPAA, "no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry."[50] The purpose of HIPAA is to develop regulations protecting the privacy and security of certain health information.[51] There are

---

cial institution' to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. Finally, the Commission proposes to include the definition of 'financial institution' and related examples in the Rule itself rather than cross-reference them from a related FTC rule, the Privacy of Consumer Financial Information Rule.").

[44] *Why was HIPAA Created?*, HIPAA GUIDE, www.hipaaguide.net/hipaa-for-dummies (last visited July 18, 2020). The Health Insurance Portability and Accountability Act (HIPAA) was created in 1996 to "modernize the flow of healthcare information, stipulate how PII maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and to address limitations on healthcare insurance coverage." *Id.*

[45] 6 U.S.C.A. § 101 (2016).

[46] Gramm Leach Bliley Act, 16 C.F.R § 314.1 (2020).

[47] *Id.* § 314.3.

[48] *Id.*

[49] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2012)).

[50] *Summary of the HIPAA Security Rule*, HHS, www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html, (last visited June 4, 2020).

[51] 6 U.S.C.A. § 101 (2016).

two rules in HIPAA: the "Privacy Rule" and the "Security Rule."[52] The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Rule, or Standards for the Protection of Electronic Protected Health Information, establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form.[53] A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information ("e-PHI").[54]

The Homeland Security Act ("HSA") was passed in 2002 and incorporates cybersecurity initiatives to keep critical infrastructure safe from cyber-attacks.[55] In 2018, the HSA was amended to establish a National Cybersecurity Center located in the Cybersecurity and Infrastructure Security Agency ("CISA"), a federal regulatory agency, which demonstrates a federal expansion of cybersecurity legislation and protection in the public sector.[56]

While public-sector critical infrastructure is monitored by the ISA, implementing cybersecurity controls in the private sector is a challenge. Some companies cannot afford cybersecurity best practices.[57] Large companies may have a wider attack surface, more data, and potentially high-profile targets, such as celebrity clients, and more employees whose sensitive PII is a prime target.[58] According to the United States Small Business Administration ("SBA"), small companies are still at risk even with a smaller attack surface.[59] According to a recent SBA survey, "88% of small business owners felt

---

[52] *See* HHS, *supra* note 50.
[53] *See id.*
[54] 45 C.F.R. § 164.312(a) (2013).
[55] 6 U.S.C.A. § Ch. 6.
[56] *See About CISA,* CISA, www.cisa.gov/about-cisa (last visited July 18, 2020).
[57] *Stay Safe from Security Threats*, SBA, www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats (last visited July 18, 2020) (88% of small business owners felt their business was vulnerable to a cyber-attack, yet many businesses can't afford professional IT solutions, they have limited time to devote to cybersecurity, or they don't know where to begin.).
[58] *See* Krebs, *supra* note 10.
[59] *Stay Safe from Cybersecurity Threats*, SBA, www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity,(last visited July 18, 2020) ("Small businesses are attractive targets because they have information that cybercriminals want, and they typically lack the security infrastructure of larger businesses.").

their business was vulnerable to a cyber-attack," yet "can't afford professional IT solutions . . . have limited time to devote to cybersecurity, [or] they don't know where to begin."[60] This makes a small business an easy target for hackers.[61] However, some sources show that companies and firms, on their own, "are best able to solve cybersecurity issues because they have the quickest access to information about relevant threats . . . evidence shows that private firms do, in fact, spend a lot of money securing their own assets."[62]

Outside of the sector specific SSCIA,[63] which covers the financial sector, HIPAA,[64] which covers healthcare PII, and the HSA, which focuses on preventing terrorist attacks within the United States,[65] U.S. cybersecurity law is largely based on a patchwork of state laws. The existence of HIPAA, the SSCIA, and the HSA show Congress recognizes the critical nature of cybersecurity, suggesting that there is potential for more federal regulation in the future for companies in the private sector.[66] However, employers are not completely without federal guidance when it comes to best practices for keeping employee data protected. The National Institute of Standards and Technology ("NIST"), a division of the U.S. Department of Commerce, created a voluntary NIST Cybersecurity Framework.[67] The purpose of the framework is to "help businesses of all sizes . . . reduce their cybersecurity risk and protect their networks and data."[68]

---

[60] *Id.*
[61] *Id.*
[62] Eli Durado, et al., *Economic Perspectives: Cybersecurity Policy Reforms for the 21st Century*, MERCATUS (Nov. 9, 2015), www.mercatus.org/publication/economic-perspectives-cybersecurity-policy-reforms-21st-century.
[63] 16 C.F.R § 314.1 (2020).
[64] 6 U.S.C.A. § 101 (2016).
[65] Homeland Security Act, 6 U.S.C.S. § 101 (2002).
[66] Taylor Armerding, *Don't Expect Jailed CEOs, But Wyden At Least Puts Consumer Privacy on The Table*, FORBES (Nov. 7, 2018, 1:52 PM), www.forbes.com/sites/taylorarmerding/2018/11/07/dont-expect-jailed-ceos-but-wyden-at-least-puts-consumer-privacy-on-the-table/#25c9f37b6215 ("Sen. Ron Wyden of Oregon issued a 'discussion draft' of his proposed Consumer Data Protection Act (CDPA) of 2018, which focuses on the prospect of CEOs going to prison for ten to twenty years if they fail to follow mandates for the use and protection of Americans' data.").
[67] *Understanding the NIST Security Framework*, FTC, www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework. (last visited July 18, 2020).
[68] *Id.*

The NIST framework provides an outline of industry best practices to help companies decide where to focus time and money for cybersecurity.[69] Much of the framework focuses on the roles and responsibilities for "employees, vendors, and anyone else with access to sensitive data."[70] This places some of the responsibility of safeguarding PII with employees themselves.[71] The framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.[72]

If cybersecurity litigation does arise, the only legal standard companies must follow is the "reasonably prudent cybersecurity measure."[73] This is an undefined standard which provides only basic, non-mandatory guidance to companies.[74] Typically, reasonable measures will involve cybersecurity risk assessments, training employees to be more cyber aware, and purchasing cybersecurity insurance.[75] Specifically, reasonable measures will likely include the following:

> Requiring all employees with access to personal information to use strong passwords, restricting employees' access to personal information to a "need-to-

---

[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] 1 CYBERSECURITY RESILIENCE PLANNING HANDBOOK § 2.05 at 1-2.
[73] Thomas J. Smedinghoff, *An Overview of Data Security Legal Requirements for All Business Sectors*, SSRN (Oct. 8, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323 ("Corporate legal obligations to implement security measures are set forth in an ever-expanding patchwork of generally applicable state, federal, and international laws, regulations, and enforcement actions, as well as common law duties and other express and implied obligations to provide reasonable or appropriate security for corporate data . . . these obligations apply to both regulated and non-regulated industries.").
[74] *Id.*
[75] *Cybersecurity Insurance*, CISA, https://www.cisa.gov/cybersecurity-insurance (last visited November 14, 2020) ("Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber-attacks by: (1) promoting the adoption of preventative measures in return for more coverage and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection. Many companies forego available policies, however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyberattack.").

> know" basis; training employees on basic cybersecurity measures and taking precautions; such as learning how to identify scams and not falling for phishing emails; using multi-factor authentication for remote access to personal information; and updating software and operating systems with the latest security patches.[76]

According to the FTC, these measures are considered reasonable.[77] Purchasing cybersecurity insurance is a further step companies can take to ensure that costs are covered to deal with the aftermath of a breach.[78] A breach can result in potentially astronomical expenses, such as legal fees, notification expenses, forensic expenses, data recovery costs, litigation costs, and costs of business.[79]

Voluntary cybersecurity guidelines have been effective in many instances. To increase awareness, understanding, and use of the cybersecurity framework, NIST publishes brief "success stories" on its website which aim to show how "diverse organizations use the Framework to improve their cybersecurity risk management."[80] The "success story" catalog, as of today, has published a total of eight case studies.[81] Each case study touts the helpfulness of the voluntary NIST guidelines. For example, the Israeli Consulate, a case study participant, wrote, "by choosing the NIST Framework, it was simpler to convince regulatory and legal professionals to support the method, since they knew it was well-established, tested, and implemented in many organizations around the world."[82]

The voluntary NIST guidelines are helpful. However, if companies are not mandated to adopt these guidelines, there is no guarantee a company is using reasonable cybersecurity measures to

---

[76] Adam Brouillet, *Understanding Reasonable Cybersecurity Measures*, FINANCIAL POISE (September 14, 2018), https://www.financialpoise.com/understanding-reasonable-cybersecurity-measures.
[77] *See* Armerding, *supra* note 66.
[78] 16 C.F.R § 314.1 (2020).
[79] Adam Brouillet, *The Legal Implications of Cybersecurity When Collecting Personal Information*, FINANCIALPOISE (Aug. 14, 2018), www.financialpoise.com/when-collecting-personal-information.
[80] *Success Stories*, NIST, www.nist.gov/cyberframework/success-stories (last visited May 31, 2020).
[81] *Id.*
[82] *Id.*

protect employee data.[83] According to Benjamin Dean, a Technology Exchange Fellow at the Center for Democracy and Technology in Washington, DC, many companies have little financial incentive to invest in cybersecurity.[84] In Dean's opinion, the financial incentives for companies to invest in greater information security are low, and government intervention might be needed.[85]

Because some companies can factor the cost of a data breach and resulting lawsuits into the cost of doing business, employee and customer data remain vulnerable.[86] The lack of incentive to invest in cybersecurity is compounded by the fact that the Cybersecurity Information Sharing Act of 2015 grants a company immunity from a lawsuit if the company volunteers information about a data breach.[87] Congress's reasoning for this immunity was to "promote the timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats."[88] Without a change in policy, companies have the option to skimp on cybersecurity, and even a way to avoid a lawsuit under CISA.

---

[83] *See* CYBERSECURITY RESILIENCE PLANNING HANDBOOK, *supra* note 72.

[84] *Why Some Companies Don't Invest in Cybersecurity*, COLUMBIA MAGAZINE (Fall 2015), https://magazine.columbia.edu/article/why-some-companies-dont-invest-cybersecurity. In recent years the cost to Target of its breach is characteristic: "the company spent $252 million afterward investigating the breach, repairing its network, and settling customers' lawsuits, but recovered most of its losses in insurance reimbursements and tax reductions that are available to companies victimized by fraud. Ultimately, Target absorbed just $105 million in damage . . . less than 0.1 percent of the company's annual revenue." *Id.*

[85] *Id.*

[86] *Id.*

[87] *Federal Cybersecurity Information Sharing Act Signed into Law*, DATA PROTECTION REPORT, (Jan. 3, 2016), https://www.dataprotectionreport.com/2016/01/federal-cybersecurity-information-sharing-act-signed-into-law. In order to receive full immunity from government and private lawsuits and other claims that may arise out of CISA-compliant monitoring, the information-sharing must be done in a manner consistent with the means specified by DHS in its Guidance. *Id.*

[88] Cybersecurity Information Sharing, 6 U.S.C § 1501.

III. WHAT A PLAINTIFF NEEDS FOR STANDING TO SUE

A threshold question in most security breach putative class action suits filed in federal court is standing.[89] The Constitution limits the judicial power of the federal courts to actual cases and controversies.[90] To establish Article III standing, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision."[91]

A major issue in data breach actions is the threat of future harm and whether it is traceable to the conduct of the defendant.[92] These cases all have something in common: a person's (or group of persons') sensitive data (such as PII or credit card numbers) were stolen from a company or employer via a cyber-attack.[93] The attackers are an invisible enemy, most likely based overseas,[94] so it is difficult to pursue the cyber criminals themselves.[95]

Customers in a putative class action tend to sue the retail establishment for allowing the data breach to occur.[96] The companies from which the data were stolen are simultaneously the victim and the defendant because employers are potentially to blame for not taking reasonably prudent cybersecurity measures before the breach occurred.[97] The employees whose data has been compromised (the plaintiffs in the action) are now under another threat – that their data

---

[89] Gerald E. Arth, George J. Krueger, & Ryan T. Becker, Fox Rothschild LLP, with Practical Law Litigation, *Non-Statutory Grounds for Challenging Class Actions: Standing and Ascertainability*,*in* PRACTICAL LAW PRACTICE NOTE 5-606-5912.
[90] U.S. CONST. art. III, § 2, cl. 1.
[91] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
[92] *See* AFG v. OPM , 928 F.3d 42 (D.C. Cir. 2019).
[93] *See* cases cited *supra* note 19.
[94] *See* Sharma, *supra* note 15.
[95] *See id.*
[96] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 (7th Cir. 2015). Customers who held department store credit cards brought putative class action against the department store, after their credit card numbers were stolen during a cyberattack, alleging negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws. *Id.*
[97] *See* AFG v. OPM, 928 F.3d 42 (D.C. Cir. 2019).

will be used for criminal purposes in the future.[98] The litigation will center around whether the threat of a potential future harm is enough for Article III standing.[99] The Federal District Circuits are split on the issue.

Twombly, *Iqbal*, and *Clapper* are three seminal Supreme Court cases that hold a future risk of harm is too remote to establish standing under Article III.[100] The sections below explore each case in detail.

A. Bell Atlantic Corp. v. Twombly

In *Twombly*, consumers brought a putative class action against incumbent local exchange carriers ("ILECs") alleging anti-trust conspiracy.[101] "The United States District Court for the Southern District of New York dismissed the complaint for failure to state a claim upon which relief can be granted."[102] The United States Court of Appeals for the Second Circuit reversed.[103] The Supreme Court granted certiorari and held as follows:

> While a complaint attacked by a Rule 12(b)(6) motion to dismiss a motion to dismiss does not need detailed factual allegations, a plaintiff's obligation to provide the "grounds" of his "entitle[ment] to relief" requires more than labels and conclusions, and a formulaic rec-

---

[98] *Id.*

[99] Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992). Article III of the Constitution confines the federal courts to adjudication of actual "cases" and "controversies." *Id.* at 559. The irreducible constitutional minimum of standing contains three elements. *Id.* at 560. First, the plaintiff must have suffered an "injury in fact," an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not "conjectural" or "hypothetical." *Id.* (citations omitted). Second, there must be a causal connection between the injury and the conduct complained of, the injury has to be "fairly . . . traceable to the challenged action of the defendant, and . . . not the result of the independent action of some third party not before the court." *Id* (quoting Simon v. Eastern Ky. Welfare Rights Org. 426 U.S. 26, 41-42 (1976). Third, it must be "likely," as opposed to merely "speculative," that the injury will be "redressed by a favorable decision." *Id.* at 561.

[100] Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007); Ashcroft v. Iqbal, 556 U.S. 662 (2009); Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

[101] *See* 550 U.S. 544.

[102] *Id.* at 552.

[103] *Id.* at 553.

> itation of the elements of a cause of action will not do.[104]

For a pleading to withstand a motion to dismiss for failure to state a claim, "factual allegations must be enough to raise a right to relief above a speculative level," even with the "assumption that all the allegations in the complaint are true even if doubtful in fact."[105] As long as there is more than a mere speculation of the facts, the complaint will likely survive a motion to dismiss.[106]

The plaintiffs, a class of subscribers of local telephone and high–speed internet services, claimed a conspiracy to restrain trade in violation of Section 1 of the Sherman Act.[107] The Court noted that the facts stated in the complaint were too ambiguous and were "consistent with conspiracy, but just as much in line with a wide swath of rational and competitive business strategy unilaterally prompted by common perceptions of the market."[108] Thus, the alleged facts were too speculative to meet the pleading standard.[109]

Writing for the majority, Justice Souter stated that the plaintiffs' complaint did not survive a Rule 12(b)(6) motion to dismiss for failure to state a claim upon which relief can be granted.[110] The complaint merely alluded to a possible conspiracy, but the facts stated in the complaint were "not enough to raise a right to relief above the speculative level on the assumption that all of the complaint's allegations are true."[111] Souter continued, "once a claim has been stated adequately, it may be supported by showing any set of facts consistent with the allegations in the complaint."[112] However, the complaint fell short of this pleading standard because "plaintiffs rest their §1 claim on descriptions of parallel conduct and not on any independent allegation of actual agreement among the ILECs."[113]

---

[104] *Id.* at 555 (citations omitted).
[105] *Id.*
[106] *Id.*
[107] *Id.* at 550 (quoting 15 U.S.C. §1) ("[E]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations.")).
[108] *Id.* at 554.
[109] *Id.*
[110] Fed. R. Civ. 12(b)(6).
[111] *Twombly*, 550 U.S. at 555.
[112] *Id.* at 563.
[113] *Id* at 564.

In conclusion, Justice Souter wrote, "because the plaintiffs here have not nudged their claims across the line from conceivable to plausible, their complaint must be dismissed."[114] In other words, a possible future injury is insufficient for Article III standing; it must be more imminent and likely to occur, at least at the pleading stage, to meet standing requirements. Justice Souter's concluding line was reinforced two years later in another Supreme Court case, *Ashcroft v. Iqbal*.

B. Ashcroft v. Iqbal

To survive a motion to dismiss for failure to satisfy the short and plain statement requirement, the complaint must offer more than a sheer possibility that a defendant has acted unlawfully or injured the plaintiff.[115] In *Ashcroft v. Iqbal,* the Supreme Court fortified its decision from *Twombly* that for standing a pleading must offer more than mere labels, conclusions or formulaic recitation of elements, and that the complaint needs further factual enhancement.[116] Thus, the Court raised the bar for plaintiffs to get into court at the pleading stage.[117]

The plaintiff in *Iqbal* was detained under suspicion of terrorist activities related to the September 11, 2001 attacks.[118] He brought an action against current and former government officials, alleging he was unconstitutionally confined under harsh conditions.[119] Specifically, the complaint alleged that defendants Ashcroft and Mueller were directly responsible for the harsh punishments and conditions of Iqbal's imprisonment because the defendants were "aware of the discriminatory policy being implemented and deliberately indifferent to it."[120] The majority disagreed.

The majority found that the plaintiff's complaint failed to plead sufficient facts to state a claim for purposeful and unlawful discrimination and that, while the claims were plausible, the facts fell

---

[114] *Id.* at 570.
[115] Ashcroft v. Iqbal, 556 U.S. 662, 662 (2009).
[116] *See id.*
[117] *See id.*
[118] *Id.* at 667.
[119] *Id.* at 668. Iqbal filed a *Bivens* action against numerous federal officials, including petitioner Ashcroft, the former Attorney General, and petitioner Mueller, the Director of the Federal Bureau of Investigation (FBI). *See id.*
[120] *Id.* at 695 (Souter, J., dissenting).

short of probable.[121] Writing for the majority, Justice Kennedy, joined by Justices Alito, Scalia, Roberts, and Thomas, explained that the complaint did not confer standing because, "while legal conclusions can provide the framework of a complaint, they must be supported by factual allegations. When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief."[122] Kennedy continued, "we begin our analysis by identifying the allegations in the complaint that are not entitled to the assumption of truth."[123] Justice Kennedy wrote that the plaintiff's complaint did not confer standing because it only listed "assertions, much like the pleading of conspiracy in *Twombly,*" which therefore, "amount to nothing more than a formulaic recitation of the elements of a constitutional discrimination claim."[124]

Next, the Court considered whether the factual allegations in respondent's complaint plausibly suggest an entitlement to relief.[125] The majority held the allegations did not surpass plausibility and reach a level of probability:

> Taken as true, these allegations are consistent with petitioners' purposefully designating detainees of high interest because of their race, religion, or national origin. But given more likely explanations, they do not plausibly establish this purpose.[126]

To reach a level of probability sufficient to confer standing, the complaint needed to contain facts "plausibly showing that petitioners purposefully adopted a policy of classifying post–September–11 detainees as of 'high interest' because of their race, religion, or national origin."[127] In sum, the Court held that the plaintiff's complaint failed to plead sufficient facts to state a claim for purposeful and unlawful discrimination against petitioners Ashcroft and Mueller.[128]

---

[121] *Id.* (Souter, J., dissenting) ("Iqbal's complaint fails to plead sufficient facts to state a claim for purposeful and unlawful discrimination.").
[122] *Id.* at 679.
[123] *Id.*
[124] *Id.*
[125] *Id.* at 681.
[126] *Id.*
[127] *Id.* at 683.
[128] *Id.* at 687.

Writing for the dissent, joined by Justices Ginsburg, Breyer, and Stevens, Souter argued that the majority misapplied the *Twombly* decision.[129] Justice Souter wrote:

> *Twombly* does not require a court at the motion-to-dismiss stage to consider whether the factual allegations are probably true. We made it clear, on the contrary, that a court must take the allegations as true, no matter how skeptical the court may be . . . The sole exception to this rule lies with allegations that are sufficiently fantastic to defy reality as we know it: claims about little green men, or the plaintiff's recent trip to Pluto, or experiences in time travel. That is not what we have here. Under *Twombly,* the relevant question is whether, assuming the factual allegations are true, the plaintiff has stated a ground for relief that is plausible. That is, in *Twombly* 's words, a plaintiff must "allege facts" that, taken as true, are "suggestive of illegal conduct."[130]

According to the minority, a court should accept facts as true unless they are so unbelievable as to suggest something scientifically or historically impossible, such as little aliens, time-travel, or interplanetary journeys.[131]

A main issue with data breach cases is whether a plaintiff has standing based on a future harm that has yet to occur. When it comes to a data breach, it is easy enough to accept facts of a complaint as true, in that cybersecurity preventions were breached, and data were stolen. However, the majority in *Iqbal* would likely hold that an impending harm due to a data breach fails to cross from the realm of plausibility into the realm of probability. While the minority in *Iqbal* would argue that harm from a data breach is not as unbelievable as "little green men," the burden remains with the plaintiff to show harm, or harm that is probably going to occur. A mere plausibility fails the test under *Iqbal*. Issues surrounding speculative and future harm are examined more closely in the Supreme Court case *Clapper.*

---

[129] *Id.* at 695-96 (Souter, J., dissenting).
[130] *See id.* at 695-96 (Souter, J., dissenting).
[131] *Id.* at 696 (Souter J., dissenting).

C. Clapper v. Amnesty International USA

The Court in *Clapper* held that allegations of "possible future injury" are not sufficient.[132] To justify standing based on future harm, the threatened injury must be "certainly impending" to constitute injury in fact.[133] This ruling has strongly influenced the interpretation of standing in data breach cases because of the similarity in the nature of the complaints and speculative injuries of the plaintiffs in *Clapper* and the plaintiffs in data breach litigation cases.[134]

In *Clapper,* the Supreme Court held the plaintiffs did not have standing to challenge the Foreign Intelligence Surveillance Act of 1978.[135] Plaintiffs were attorneys and human rights, labor, legal, and media organizations whose work required them to engage in "sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad."[136] They feared their communications with their foreign contacts would be intercepted under § 1881a "at some point in the future."[137]

---

[132] Clapper v. Amnesty Int'l, 568 U.S. 398, 409 (2013).
[133] *Id.* at 410-14.
[134] *See, e.g.*, Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) (holding that *Clapper* does not suggest that the certainly impending standard is limited to the national security context or that it does not apply generally to the standing analysis); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 654 (S.D. Ohio 2014) (holding that an increased risk of identity theft, identity fraud, medical fraud or phishing is not itself an injury-in-fact because Named Plaintiffs did not allege—or offer facts to make plausible—an allegation that such harm is certainly impending); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 875 (N.D. Ill. 2014) (holding that under *Clapper*, to the extent the plaintiff's alleged injuries are premised on the mere possibility that her [personal identifying information] was stolen and compromised, and a concomitant increase in the risk that she will become a victim of identity theft, [the plaintiff]'s claim is too speculative to confer Article III standing); *In re* SAIC, 2014 WL 1858458, at 9 (holding that under *Clapper*, increased risk of harm alone does not constitute an injury in fact. Nor do measures taken to prevent a future, speculative harm); *In re* Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 WL 4759588, at 5 (N.D. Ill. Sept. 3, 2013) (holding that under *Clapper*, the plaintiffs' claim of actual injury in the form of increased risk of identity theft is insufficient to establish standing because speculation of future harm does not constitute actual injury).
[135] 50 U.S.C.A. § 1881a.
[136] *Clapper*, 568 U.S. at 406.
[137] *Id.*

Plaintiffs based their complaints on two assertions.[138] First, they relied on communications with individuals outside the United States who "were likely to be the targets of surveillance under section 702," and the surveillance of these individuals made it likely that their communications would be intercepted.[139] In other words, the plaintiffs argued that the government must have been targeting individuals outside the U.S., and this government action opened up the possibility the plaintiffs' conversations might be overheard. Second, plaintiffs claimed they would suffer ongoing injuries that are fairly traceable to §1881a because the risk of §1881a surveillance requires them to take costly and burdensome measures to protect the confidentiality of their communications.[140]

The Court characterized the plaintiffs' fear of having their conversations overheard as "highly speculative" given that the respondents did not allege that any of their communications had actually been intercepted, or even that the U.S. Government sought to target them directly.[141] Writing for the majority, Justice Alito stated the plaintiffs failed to demonstrate the future injury they purportedly feared was "certainly impending."[142]

The Court reasoned that a future injury was not certain in *Clapper* because the plaintiffs' standing theory rested on a "speculative chain of possibilities that does not establish that their potential injury is certainly impending or is fairly traceable."[143] The Court explained why the complaint was too speculative in a five-pronged argument:

> First, it is highly speculative whether the Government will imminently target communications to which respondents are parties . . . their theory necessarily rests on their assertion that their foreign contacts will be targeted. Yet they have no actual knowledge of . . . targeting practices. Second, even if respondents could demonstrate that the targeting of their foreign contacts is imminent, they can only speculate as to whether the Government will seek to use § 1881a-authorized sur-

[138] *Id.*
[139] *Id.*
[140] *Id.* at 410.
[141] *Id.*
[142] *Id.*
[143] *Id.*

> veillance . . . Third, even if respondents could show that the Government will seek FISC authorization to target respondents' foreign contacts under § 1881a, they can only speculate as to whether the FISC will authorize the surveillance . . . Fourth, even if the Government were to obtain the FISC's approval to target respondents' foreign contacts under § 1881a, it is unclear whether the Government would succeed in acquiring those contacts' communications. And fifth, even if the Government were to target respondents' foreign contacts, respondents can only speculate as to whether their own communications with those contacts would be incidentally acquired.[144]

The complaint also stated that the plaintiffs would have to make expenditures to protect themselves from harm resulting from the surveillance.[145] This too, the Court said, was based on a "hypothetical future harm that was not certainly impending," and concluded the respondents were attempting to "manufacture standing."[146] This argument is critical in understanding how the lower courts have interpreted the claims of plaintiffs in data-breach lawsuits. A "chain of events" analogy relates to the speculation by plaintiffs that there is a possibility their PII will be used for fraud or identity theft in the future.[147]

Clapper held that an injury must be either "present" or "certainly impending" to confer standing.[148] *Clapper* also held that an attenuated chain of possibilities does not confer standing and that plaintiffs cannot create standing by taking steps to avoid an otherwise speculative harm.[149] Thus, the threshold for establishing standing

---

[144] *Id.*
[145] *Id.* at 398. Plaintiffs are lawyers, journalists, human rights researchers, and others whose communications are very likely to be monitored under the Act and who, in reasonable response to the substantial risk of surveillance under the FAA, and in order to comply with rules of professional conduct, have been compelled to take costly and burdensome measures to protect the confidentiality of information that is sensitive or privileged. *See id.* at 415, 426-427.
[146] *Id,* at 402("Respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending.").
[147] *See* Wright, *supra* note 11.
[148] *Clapper*, 568 U.S. at 401.
[149] *Id.* at 410.

based on injuries that have yet to occur – such as identity theft after a data breach is high.

IV. THE CIRCUIT SPLIT INVOLVING STANDING IN DATA BREACH CASES

A. The Second, Third, and Fourth Circuits hold that the risk of injury due to a data breach is too speculative to confer standing.

The District Court in *Whalen v. Michaels Stores, Inc.* [150] and in *Steven v. Carlos Lopez & Assocs., LLC*[151] held that a future risk of identity theft after a data breach does not confer standing. The Second Circuit was joined by the First Circuit in *Katz v. Pershing, LLC*,[152] the Third Circuit in *Reilly v. Ceridian Corp.,*[153] and the Fourth Circuit in *Beck*.[154] This section will compare the Second Circuit cases *Whalen,* and *Steven v. Carlos Lopez & Assocs.* with the Third Circuit's decision in *Reilly v. Ceridian Corp.*.

The District Court held in *Whalen* that there was no plausible risk of future harm when plaintiff's credit card information was stolen.[155] The plaintiff, Ms. Whalen, claimed breach of implied contract and deceptive acts after her personal credit card information was stolen from the store in a security breach.[156] Whalen made purchases with her credit card at a Michaels retail location during the time of the breach.[157] Whalen was joined in a class action by other customers whose data were also compromised in the breach.[158] Michaels Stores, the defendant, confirmed the existence of the security breach.[159] As a result, Michaels offered free credit monitoring ser-

---

[150] 153 F. Supp. 3d 577 (E.D.N.Y. 2015), *aff'd* 689 F. App'x 89 (2d Cir. 2017).
[151] 422 F. Supp. 3d 801 (S.D.N.Y. 2019).
[152] 672 F.3d 64, 69 (1st Cir. 2012).
[153] 664 F.3d 38 (3d Cir. 2011).
[154] 848 F.3d 262 (4th Cir. 2017).
[155] *See* Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577 (E.D.N.Y 2015).
[156] *Id.* at 578.
[157] *Id.* ("Michaels estimated that approximately 2.6 million cards may have been affected during the time period between May 8, 2013 and January 27, 2014.").
[158] *Id.*
[159] *Id.* ("On January 25, 2014, Michaels initially notified its customers of possible fraudulent activity on some U.S. payment cards. Three months later, Michaels confirmed the existence of the Security Breach. Michaels reported that hackers used a highly sophisticated malware, or malicious software, to retrieve the credit and debit

vices for twelve months.[160] Whalen claimed that because hackers stole her credit card information, she suffered damages from "costs associated with identity theft" and also risked future harm.[161] Michaels moved to dismiss the Complaint under Rules 12(b)(1) for lack of subject matter jurisdiction and 12(b)(6) for failure to state a claim.[162]

The court held for the defendant because it concluded Whalen lacked Article III standing.[163] The court analyzed whether Whalen and the class had suffered an actual injury in fact or an imminent injury.[164] In the class action context, plaintiffs must show that they "personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong."[165] Whalen did not face risk of actual harm, and she did not sustain any unreimbursed charges.[166] The court also held that credit monitoring expenses were not a recognized harm.[167] The Supreme Court dismissed this type of harm in *Clapper* when it stated "if the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear."[168]

Whalen made two other arguments which also failed.[169] First, Whalen claimed that she "reasonably expected her data would be safeguarded" when she made purchases at Michaels Stores.[170] How-

---

card information from the systems of Michaels stores and its subsidiary, Aaron Brothers . . . there was no evidence that the hackers retrieved any other customer information, such as names, addresses, or PIN numbers.").

[160] *Id.*

[161] *Id.* at 579 ("Whalen asserts that she has suffered damages arising out of costs associated with identity theft and the increased risk of identity theft, But, she concedes that fraudulent use of cards might not be apparent for years.").

[162] *Id.*

[163] *Id.*

[164] *Id.* at 580 ("To establish standing under Article III of the Constitution, a plaintiff must show that the injury-in-fact is: (1) concrete, particularized, and actual or imminent; (2) fairly traceable to the defendant's conduct; and (3) redressable by a favorable court decision").

[165] *Id.* (quoting Warth v. Seldin, 422 U.S. 490, 503(1975)).

[166] *Id.*

[167] *Id.* at 581 ("[T]he Supreme Court has dismissed this type of argument, explaining that plaintiffs cannot 'manufacture standing' through credit monitoring" (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2013)).

[168] *Id.* (quoting *Clapper*, 133 S. Ct. at 1151).

[169] *Id.*

[170] *Id.* at 581.

ever, because a customer is not charged more to pay with a credit card instead of another payment method, such as cash, the court found that this argument failed.[171] Second, Whalen alleged that her credit card lost value after the breach.[172] The court found that Whalen failed to allege how her credit card information or PII became less valuable, and instead merely asserted that "[c]onsumers . . . place economic value on the ability to restrict improper access to their personal information."[173] With no specific allegations about how her cancelled credit card information lost value, Whalen lacked standing on this ground as well.[174]

In *Steven v. Carlos Lopez & Assocs.*, employees brought a class action against their employer alleging that employee data were compromised by an "errant email sent within employer."[175] The Southern District confirmed that, even though the company accidentally sent out the PII of 130 employees in an email blast to customers, the plaintiffs lacked Article III standing because there was no concrete or imminent injury-in-fact.[176] The court noted that other courts have held that the theft of PII in a data breach gives plaintiffs the standing to bring claims "against the entity that had held their data based on an increased risk of future identity theft."[177] The major difference in the success of a claim goes beyond the circuit where the

---

[171] *Id.*

[172] *Id.*

[173] *Id.* at 582.

[174] *Id.* The court references Galaria v. Nationwide Mut. Ins. Co. 998 F. Supp. 2d 646, 660 (S.D. Ohio 2014), which also dismissed an argument that a plaintiff's PII lost value in a data breach because the plaintiffs did not allege any facts to support their position. *Id.*

[175] Steven v. Carlos Lopez & Assocs., LLC. 422 F. Supp. 3d 801, 806 (S.D.N.Y. 2019). Carlos Lopez & Associates (CLS), the defendant and employer, accidentally sent an email containing personal information about approximately 130 current and former CLA employees to a distribution list of current CLA employees. *Id.*

[176] *Id.* at 804 ("Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes.").

[177] *Id. See e.g., In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 55-61 (D.C. Cir. 2019) ("OPM"); Attias v. Carefirst, Inc., 865 F.3d 620, 628-29 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 387-89 (6th Cir. 2016) (unpublished); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967-68 (7th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692, 694-95 (7th Cir. 2015); Fero v. Excellus Health Plan, Inc., 304 F. Supp. 3d 333, 338-40 (W.D.N.Y. 2018); Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 746 (S.D.N.Y. 2017).

plaintiffs bring suit. In several of these cases, "at least one named plaintiff alleged actual misuse of his or her personal information by the suspected data thief."[178] When a criminal actually misused stolen information, the injury was concrete enough to confer Article III standing.[179] Also, during oral arguments, plaintiffs "could not name a single case in which a court had found standing based on the risk of future identity theft that did not arise from . . . an intentional act" on the part of the hacker.[180]

The Third Circuit in *Reilly v. Ceridian Corp.* held that a breach at a payroll processing firm did not confer standing for plaintiffs to sue.[181] Plaintiffs were law firm employees who brought a class action against Ceridian Corporation, alleging various claims, including negligence and breach of contract relating to increased risk of identity theft and costs to monitor credit activity after a firm suffered a security breach, as well as a claim for emotional distress.[182] The lower court dismissed for lack of standing and failure to state a claim.[183] The Court of Appeals held that the allegations were insufficient to plead actual injury.[184]

B. The Sixth, Seventh, Ninth, Eleventh, and D.C. Circuits hold that the risk of injury due to a data breach is sufficient to confer standing.

In *Attias v. Carefirst, Inc.*,[185] the D.C. Circuit held that the plaintiffs had standing to sue their health insurer after a cyber-attack in which hackers stole PII in the form of social security numbers, credit card numbers, and health care information.[186] In *Lewert v. P.F. Chang's China Bistro, Inc.*, the Seventh Circuit also held that the plaintiffs had standing to sue when their credit card information alone was breached.[187] The Seventh Circuit and the D.C. Circuit were

---

[178] *Carlos Lopez,* 422 F.Supp at 804.
[179] *Id.*
[180] *Id.*
[181] *See* Reilly v. Ceridian Corp, 664 F.3d 38 (3d Cir. 2011).
[182] *Id.* at 40.
[183] *Id.*
[184] *Id.*
[185] 865 F.3d 620 (D.C. Cir. 2017).
[186] *Id.* at 622.
[187] *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016).

joined by the Sixth Circuit in *Galaria v. Nationwide Mut. Ins. Co.*,[188] the Ninth Circuit in *Krottner v. Starbucks Corp.*[189] and in *Ree v. Zappos.com, Inc.* (*In re Zappos.com, Inc.*).[190] Each of these cases held that the risk of injury due to a data breach is sufficient to confer standing.[191] This section will compare the *Attias* and *Lewert* cases in more detail.

The D.C. Circuit in *Attias* was primarily concerned with the injury-in-fact requirement of Article III standing.[192] There, health insurer CareFirst suffered a cyberattack in 2014 in which its customers' personal information was allegedly stolen.[193] In a class action, a group of CareFirst customers attributed the breach to the company's carelessness and sued.[194] The District Court dismissed for lack of standing, finding the risk of future injury to the plaintiffs too speculative to establish injury in fact.[195] The D.C. Circuit reversed, holding that the plaintiffs "cleared the low bar to establish their standing at the pleading stage."[196]

The plaintiffs in *Attias* alleged that a data breach at CareFirst exposed them to a heightened risk of identity theft.[197] The company stored customer PII on its servers.[198] Allegedly, CareFirst failed to properly encrypt some of the data and left the PII of its customers vulnerable to a cyber-attack.[199] While the court agreed that the plaintiffs failed to meet the "certainly impending" test set forth in *Clapper*, the court found that the plaintiffs met the burden of showing a sub-

---

[188] 663 F. App'x 384 (6th Cir. 2016). The court found Article III standing "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in plaintiffs' complaints." *Id.* at 388.

[189] 628 F.3d 1139 (9th Cir. 2010) (holding that plaintiffs sufficiently alleged standing based on the risk of identity theft).

[190] 888 F.3d 1020 (9th Cir. 2018) (holding that plaintiffs sufficiently alleged an injury in fact under *Krottner*, based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft).

[191] *See, e.g.,* Krottner v. Starbucks, 628 F.3d 1139 (9th Cir. 2010); Ree v. Zappos.com, 888 F.3d 1020 (9th Cir. 2018); In re 21st Century Oncology Customer Data Sec. Breach Litig., 380 F. Supp. 3d 1243 (M.D. Fla. 2019).

[192] Attias v. CareFirst, Inc., 865 F.3d 620 (2017).

[193] *Id.* at 622.

[194] *Id.*

[195] *Id.*

[196] *Id.*

[197] *Id.* at 623.

[198] *Id.*

[199] *Id.*

stantial risk of impending injury set forth in *Susan B. Anthony List v. Driehaus*.[200]

In *Attias*, the court found that a plaintiff could establish standing by satisfying one of two tests.[201] The first test was the "certainly impending" test; the second was the "substantial risk" test.[202] The complaint must also have plausibly alleged that the plaintiffs faced "a substantial risk of identity theft as a result of CareFirst's alleged negligence in the data breach."[203] This holding turned on the lower court's erroneous finding that that the complaint "did not allege the theft of social security or credit card numbers in the data breach."[204] Because the hackers had access to so much PII – including social security numbers, credit card numbers, and personal health information – the court reasoned that the risk of identity theft was heightened, and also noticed a difference between these facts and those of *Clapper*.[205] Citing precedent from the D.C. Circuit,[206] the court held "the proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm" as long as the harm is "fairly traceable to the challenged conduct of the defendant."[207] This is distinguishable from *Clapper*, in which the Supreme Court emphasized that, to establish Article III standing, a future injury must be certainly impending, rather than simply speculative.[208]

---

[200] 573 U.S. 149 (2014). Plaintiffs challenged an Ohio statute that prohibited certain "false statements" during the course of a political campaign. *See Id.*

[201] Attias, 865 F.3d at 626–27.

[202] *Id.*

[203] *Id.* at 627.

[204] *Id.* ("The complaint alleged that CareFirst, as part of its business, collects and stores its customers' personal identification information, personal health information, and other sensitive information, all of which the plaintiffs refer to collectively as 'PII/PHI/Sensitive Information . . . This category of PII/PHI/Sensitive Information . . . includes patient credit card . . . and social security numbers.'").

[205] *Id.* at 628 ("Our conclusion that the alleged risk here is 'substantial' is bolstered by a comparison between this case and the circumstances in *Clapper* . . . here . . . an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative—at the very least, it is plausible—to infer that this party has both the intent and the ability to use that data for ill.").

[206] *See, e.g.*, *In re* Idaho Conservation League, 811 F.3d 502, 509 (D.C. Cir. 2016) (using "significant risk" and "reasonable fears" as the standard); Nat'l Ass'n of Broadcasters v. FCC, 789 F.3d 165, 181 (D.C. Cir. 2015) (using "substantial risk"); Sierra Club v. Jewell, 764 F.3d 1, 7 (D.C. Cir. 2014) (using "substantial probability of injury").

[207] *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016)).

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

In *Lewert v. P.F. Chang's China Bistro, Inc.*, the Seventh Circuit also considered whether a plaintiff satisfies the standing criteria imposed by Article III of the Constitution.[209] This was not the Seventh Circuit's first time it looked at standing in a case involving a data breach.[210] The court found that plaintiffs did have standing to sue.[211]

The defendant, P.F. Chang's China Bistro, acknowledged that it experienced a data breach in June of 2014.[212] As a result of this breach, the plaintiffs sued due to an "increased risk of fraudulent charges and identity theft, because their data has already been stolen."[213] The court held that this was enough to confer Article III standing, citing *Remijas v. Neiman Marcus Grp.*, which held "it is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is sooner or later to make fraudulent charges or assume those consumers' identities."[214]

The language "sooner or later" seems to contradict the very definition of Article III standing that was upheld in *Clapper*.[215] The court in *Lewert* reconciled this difference because in *Clapper*, the plaintiffs alleged a possible future injury based on a fear that the government *might* have intercepted their private communications when no such interception had yet occurred.[216] In contrast, the court stated that since the data breach had already occurred, this was sufficient to give plaintiffs standing.[217] Specifically, the data breach already led to two potential future injuries that this court held were sufficiently im-

---

[209] *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016).
[210] *Id.* at 966 ("Neiman Marcus experienced a data breach that poten-tially[sic] exposed the payment-card data of all customers who paid with cards during the previous year . . . [plaintiffs] brought a class action based on the breach. We concluded that several of those plaintiffs' injuries were concrete and particularized enough to support Article III standing.").
[211] *Id.*
[212] *Id.* at 967.
[213] *Id.*
[214] *Id.* (quoting Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015)).
[215] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (holding that to establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling).
[216] *See* Lewert, 819 F.3d 963.
[217] *Id.*

minent: the increased risk of fraudulent credit- or debit-card charges, and the increased risk of identity theft.[218]

Notably, the court in *In Re Zappos* also distinguished the standing needed in a data breach case with the standing requirements found in *Clapper*.[219] The court wrote, "*Clapper's* standing analysis was especially rigorous because the case arose in a sensitive national security context . . . and because the plaintiffs were asking the courts to declare actions of the executive and legislative branches unconstitutional."[220] Distinguishing *Clapper* for being based in a national security context, the court relied on the Ninth Circuit decision *Krottner v. Starbucks Corp.*. In *Krottner*, the court held that that employees of Starbucks had standing to sue the company based on the "risk of identity theft they faced after a company laptop containing their personal information was stolen."[221] However, the Supreme Court in *Clapper* did not rely on the national security aspect of the case to decide the case. The Court did not imply or state that standing should be more rigorous in a national security context. The Supreme Court instead relied on cases that did not relate to national security issues to determine that the plaintiffs lacked Article III standing in *Clapper*.[222] Therefore, the distinction about a national security context by the court in *In Re Zappos* is based on the differences in the facts of *Clapper*, not the reasoning for the holding by the Supreme Court.

The cyber-attacks in *Remijas*[223] and in *Lewert* had already occurred when the plaintiffs brought their suits. In contrast, the plaintiffs sued in *Clapper* based on fear of an action that had not yet occurred (government interception of phone calls).[224] This is a major difference. However, to say that this difference alone can allow Article III standing in a data breach is overbroad. There is no certainty that, just because data has been stolen, it will definitely be used by hackers.[225] The term "sooner or later" does not imply an imminent harm that is scheduled to occur. If people could sue because sooner or later they would be injured, it would open up a floodgate of frivo-

---

[218] *Id.* at 691–94.
[219] *In re* Zappos.com, Inc., 888 F.3d 1020 at 1026.
[220] *Id.* (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013)).
[221] Krottner v. Starbucks Corp., 628 F.3d 1139, 1140, 1143 (9th Cir. 2010).
[222] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
[223] 794 F.3d 688 (7th Cir. 2015).
[224] *Clapper*, 568 U.S. at 408.
[225] *Id.*

lous lawsuits. Sooner or later, every person "might" be harmed because of any number of hypotheticals.

As data privacy law progresses and the courts see more cases about PII being stolen, we might see a trend that shows that PII is harder to trace and potentially more valuable than mere Credit Card (CC) information. The case law tells us there is an emerging difference for what will fulfill the imminent harm Article III standing requirement when only credit card information has been stolen versus when PII has been stolen. After a breach at a retail establishment, a credit card company alerts a consumer to potentially fraudulent activity.[226] Certainly, the PII of wealthy clients or government agents is extremely valuable for hackers.[227] There is data that show healthcare PII is far more valuable than a credit card number.[228] But for now, "sooner or later" is still not good enough to confer standing in half of the United States Circuit Courts.

V. DATA BREACH CASES INVOLVING EMPLOYEE DATA

A narrow issue presents itself in cases when employee data is stolen from human resources at a place of employment. Currently, there is no federal legislation that protects employees in the event of a breach at their place of work. This section focuses on cybersecurity cases involving employee data and the burden placed on employers to keep their employees' data safe from breaches.[229]

---

[226] *See, e.g.,* Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577 (E.D.N.Y. 2015) (Plaintiff's credit card company alerted her that there were fraudulent charges on her card.).

[227] *How Much Is Your Data Selling For On The Dark Web?*, EXPERIAN.COM, www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web (last visited July 18, 2020). The value data of data changes and is affected by many factors including supply and demand but here are the 10 most common pieces of information sold on the Dark Web and the general range of what they're worth: Social Security number – $1, Online payment services information – $20 – $200, Credit or debit card info – $5 – $110, Driver's license – $20, Loyalty accounts – $20, Diplomas – $100 – $400, Passports – $1000 – $2000, Subscription services – $1 – $10, Medical records – $1 – $1000, General logins – $1. *Id.*

[228] *See id.*

[229] Employers store employee PII and it can be vulnerable to hackers. This Note analyzes the intersection of laws relating to a duty of companies to take reasonably prudent cybersecurity standards to protect data, and any laws that show a duty owed to employees, exposing the lack of regulations that compel companies and employers to protect the PII of employees.

In July of 2015, the National Treasury Employees Union ("NTEU") filed a class action lawsuit against the United States Office of Personnel Management ("OPM"), the federal government's chief human resources agency. [230] The NTEU was joined by the American Federation of Government Employees in the action, on behalf of individual plaintiffs and a putative class of others similarly affected by the breaches (the "Arnold Plaintiffs").[231] According to OPM's website, "approximately 21.5 million individuals were impacted by the cyber incident involving background investigation records" and "approximately 4.2 million individuals were impacted by the separate but related cyber incident involving personnel records."[232] The OPM maintained electronic personnel files that contain PII of employees, and also oversaw "more than two million background checks and security clearance investigations per year."[233]

After hackers breached its human resources database, OPM moved to dismiss, arguing that plaintiffs lacked Article III standing and that plaintiffs' complaints were barred by sovereign immunity.[234] Co-defendant KeyPoint investigators, a third-party government contractor that had access to OPM's database, also moved to dismiss for failure to state a claim.[235] The District Court dismissed for lack of Article III standing and failure to state a claim.[236]

On appeal, in *AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.)*, the D.C. Circuit reversed in part and held that both sets of plaintiffs alleged facts sufficient to satisfy Article III standing requirements.[237] The court agreed with the lower court that

---

[230] *In re* United States OPM Data Sec. Breach Litig., 266 F. Supp. 3d 1 (D.D.C. 2017).
[231] *Id.*
[232] *Cybersecurity Resource Center*, OPM, www.opm.gov/cybersecurity (last visited July 18, 2020).
[233] OPM, 266 F. Supp. At 50To facilitate these investigations, OPM collects a tremendous amount of sensitive personal information from current and prospective federal workers, most of which it then stores electronically in a "Central Verification System." *Id.*
[234] *Id.*
[235] *Id.*
[236] *Id.* (holding that the fact that a plaintiff's data was taken was not enough by itself to create standing to sue and plaintiffs did not plead sufficient facts to demonstrate economic loss or that any alleged injuries were fairly traceable to defendants' actions).
[237] AFGE v. OPM (*In re* United States OPM Data Sec. Breach Litig.), 928 F.3d 42 (D.C. Cir. 2019).

NTEU plaintiffs did not sufficiently allege a violation of a "constitutional right to privacy."[238] This section will examine why the plaintiffs met the requirements of Article III standing in this case, and also the implications of the failure to meet a constitutional right to privacy in a data breach case.

The *AFGE v. OPM* case is set apart because the plaintiffs stated a claim based on a breach of The Privacy Act.[239] Other data breach cases were not based on a breach of a Federal Act, because there are only a handful of sector-specific federal statutes to protect data.[240] The Privacy Act is a federal statute that states "no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[241] The term "record" is defined in the Privacy Act as the following:

> Information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.[242]

The records listed in the statute are a typical definition of PII. The Privacy Act sets out clear standards that allow for a claim to be brought.[243] These include an intent requirement that the defendant's conduct must be "intentional or willful,"[244] a causation requirement that the defendant's conduct must be the "proximate cause"[245] of the

---

[238] *Id.* at 54.
[239] 5 U.S.C. § 552a.
[240] *See*, *e.g.,* The Standards for Safeguarding Customer Information Act ("SSCIA"), the Health Insurance Portability and Accountability Act ("HIPAA"), and the Homeland Security Act ("HSA") of 2002.
[241] 5 U.S.C. §552a.
[242] *Id.*
[243] *OPM*, 928 F.3d at 62 ("The Privacy Act waives sovereign immunity by expressly authorizing a cause of action for damages against federal agencies that violate its rules protecting the confidentiality of private information in agency records.").
[244] *Id.* ("Under the Privacy Act, willfulness means more than 'gross negligence.'").
[245] *Id.* at 67. The conduct must have been a "substantial factor" in the sequence of events leading to Plaintiffs' injuries, and those injuries must have been "reasonably foreseeable or anticipated as a natural consequence." *Id.*

harm, and a damages requirement where the plaintiff(s) must suffer "actual damages."[246]

The plaintiffs alleged that OPM "willfully" violated the Privacy Act's requirements, thus meeting the Act's standard for liability.[247] The court agreed that the plaintiffs' complaint alleged sufficient facts to open the door to litigation based on OPM's willfully allowing the breach to occur, because OPM had repeatedly "failed to take basic, known, and available steps to secure the trove of sensitive information in its hands."[248] The plaintiffs met the causation requirement because the "Arnold Plaintiffs have plausibly alleged a substantial risk of future identity theft that is fairly traceable to OPM's and KeyPoint's cybersecurity failings . . . and the NTEU Plaintiffs have plausibly alleged actual and imminent constitutional injuries that are likewise traceable to OPM's challenged conduct."[249] The plaintiffs also met the "actual damages" requirement because they "suffered forms of identity theft accomplishable only with the type of information that OPM stored and the hackers accessed."[250] The court held that this directly linked the hack to the theft of the victims' private information, the pecuniary harms suffered, and the ongoing increased susceptibility to identity theft or financial injury.[251]

The OPM case stands apart from other data breach cases because of the Privacy Act. OPM was held liable because of the Privacy Act which provided a legal basis to give plaintiff's standing to bring suit.[252] Ironically, even though plaintiffs were suing a federal

---

[246] *Id.* at 64. "Actual damages" within the meaning of the Privacy Act are limited to proven pecuniary or economic harm." *Id.*

[247] *Id.* at 62 ("OPM's decisions not to comply with [Information Security Act] requirements for critical security safeguards enabled hackers to access and loot OPM's systems for nearly a year without being detected. Despite known and persistent threats from cyberattacks, OPM allowed multiple 'material weaknesses' in its information security systems to continue unabated. As a result, Plaintiffs' and Class members' [government investigation information] under OPM's control was exposed, stolen, and misused." (citations omitted)).

[248] *Id.* at 64 ("The complaint's plausible allegations that OPM decided to continue operating in the face of those repeated and forceful warnings, without implementing even the basic steps needed to minimize the risk of a significant data breach, is precisely the type of willful failure to establish appropriate safeguards that makes out a claim under the Privacy Act.").

[249] *Id.* at 61.

[250] *Id.* at 67.

[251] *Id.*

[252] *Id.*at 49 ("The Privacy Actprovides just such a waiver of sovereign immunity. That statute 'safeguards the public from unwarranted collection, maintenance, use

entity and sovereign immunity had to be waived by the meeting of three statutory elements, it was a successful claim. Without the Privacy Act protecting federal employee data, it is possible that this case would have been dismissed at the pleading stage for failure to state a claim.

VI. THE PROTECTIONS OF EMPLOYEE DATA UNDER CURRENT U.S. LAW COMPARED TO THE GDPR

Employment law is a mix of common law,[253] statutes, and regulations that are in effect to ensure that both employer and employee are treated fairly.[254] Employers owe a basic duty to their employees to maintain a safe working environment.[255] Congress passed the Occupational Health and Safety Act ("OSH-Act") with the purpose of keeping America's workforce safe and healthy for many public policy reasons.[256] However, OSH-Act set a clear standard for physical safety, it did not set a standard for the safety of employee PII. Under current U.S. law, employers owe no duty to employees to keep their data private or secure beyond the standard reasonably prudent cybersecurity measures.[257] The current standard fails to ade-

---

and dissemination of personal information contained in agency records.' As part of that obligation, the Act mandates that federal agencies 'protect the privacy of individuals identified in information systems maintained by [them].' The Privacy Act waives sovereign immunity by expressly authorizing a cause of action for damages against federal agencies that violate its rules protecting the confidentiality of private information in agency records." (citations omitted) (first quoting Henke v. United States DOCe, 83 F.3d 1453, 1456 (D.C. Cir. 1996); then quoting Pub. L. No. 93-579, § 2(a)(5), 88 Stat. 1896, 1896 (1974))).

[253] *See, e.g*., Matthew W. Finkin, *International Governance and Domestic Convergence in Labor Law as Seen from the American Midwest*, 76 IND. L. J. 143, 166 (2001) ("Despite the overlay of federal protection law … our law of employment [in the U.S.] remains overwhelmingly state law, both legislative and judge made.").

[254] *See, e.g.,* labor regulations under 29 U.S.C § 8, *and* 29 C.F.R. for federal regulations about employment.

[255] Occupational Safety and Health Administration, Employer Responsibilities, UNITED STATES DEPARTMENT OF LABOR, www.osha.gov/as/opa/worker/employer-responsibility.html (last visited November 15, 2020). Under the OSH-Act, employers have a responsibility to provide a safe workplace. *Id.*

[256] 29 U.S.C. § 651. The Congress finds that personal injuries and illnesses arising out of work situations impose a substantial burden upon, and are a hindrance to, interstate commerce in terms of lost production, wage loss, medical expenses, and disability compensation payments. *Id.*

[257] *See* Brouillet, *supra* note 24.

quately protect employees because employers are not aware that employee PII is valuable to hackers.z.[258]

Human Resources departments have access to sensitive employee data and at a minimum must follow reasonably prudent cybersecurity measures. State laws in the area of protecting employee data "are a patchwork collection and are neither uniform nor completely consistent."[259] HR professionals should note that state laws are the primary source of potential identity-theft liability for employers.[260] There is no all-encompassing federal law about protecting employee data.[261] A recent trend in state law is to expand the definition of PII:

> The Maryland General Assembly recently amended the Maryland Personal Information Protection Act to expand the definition of personal information, provide a 45-day timeframe for providing notice of a breach. . . . Maryland's data breach notification statute (Md. Code Com. Law §14-3501) [expanded the definition of PII] to include: Passport numbers and other identification numbers issued by the federal government; State identification card numbers; Health information, defined to include any information created by an entity covered by HIPAA regarding an individual's medical history, condition, treatment or diagnosis; A health insurance policy, certificate number or health insurance subscriber identification number in combination with a unique identifier that permits access to the infor-

---

[258] *Underrated Risks of Data Exposure*, TERBIUM LABS, terbiumlabs.com/resources/the-underrated-risks-of-data-exposure (last visited Oct. 30, 2020). Fewer than 11% of those surveyed believe social security numbers, names, bank accounts and payroll records of employees are the sorts of data that cyber criminals are interested in. *Id.*

[259] Lisa Nagele-Piazza, J.D, *Six Ways Employers Can Help Prevent a Data Breach*, SHRM, (Mar. 14, 2018) www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/6-ways-hr-can-help-prevent-a-data-breach.aspx. (quoting Patrick Fowler: "California and Massachusetts have been more active than other states in passing data privacy legislation, but virtually all of the states have data breach notification laws at this point . . . Employers should make sure they know what is required under relevant state laws.").

[260] Lisa Nagele-Piazza, J.D, *Employers May Be Liable For Worker Identity Theft*, SHRM, (Nov. 8, 2017) www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/employers-may-be-liable-for-worker-identity-theft.aspx.

[261] 29 U.S.C. § 651.

> mation; Biometric data, such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic that can be used to uniquely authenticate a person's identity upon accessing a system or account; A user name or e-mail address in combination with a password or security question and answer that permits access to the account. [262]

The previous version of Maryland's law only covered customer records; the amended law will cover records relating to employees and former employees that contain personal information.[263]

New York recently promulgated a cybersecurity regulation for the financial industry, "Cybersecurity Requirements for Financial Services Companies."[264] The regulation states that increased cybersecurity measures are needed in the financial vertical, because "the financial services industry is a significant target of cybersecurity threats."[265] The law also states, "it is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs."[266]

In 2018, California passed the California Consumer Privacy Act of 2018, which gives consumers more control over the personal information that businesses collect about them.[267] Under the Act, California's residents may ask businesses to disclose what personal information they have about them, and what the businesses do with that information.[268] Residents can request that businesses delete their personal information and to not sell personal information.[269] However, this law does not include the protection of employee data.[270]

---

[262] Edward J. McAndrew, David M. Stauss, Gregory Szewczyk & Ballard Spahr, *Maryland Amends Data Breach Notification Law*, SHRM (Aug. 9, 2017), www.shrm.org/ResourcesAndTools/legal-and-compliance/state-and-local-updates/pages/maryland-amends-data-breach-notification-law.aspx.
[263] *Id.*
[264] 23 NYCRR 23 § 500.0 (July 22, 2020).
[265] *Id.*
[266] *Id.*
[267] California Consumer Privacy Act, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, oag.ca.gov/privacy/ccpa (last visited October 30, 2020).
[268] *Id.*
[269] *Id.*
[270] *Id.*

Notably, the Maryland, New York, and California laws relate to consumer protection and not to the safeguarding of employee data, despite the higher price tag on the dark web of employee data compared to credit card numbers.[271] These regulations do not protect employees, or consumers, from hacking. It will be interesting to watch the evolution of other states' data protection laws and if any states will consider a statute explicitly protecting employee PII.

In 1995, the European Union worked to "harmonize EU privacy law" by passing a directive.[272] This was similar to the NIST framework that exists in the United States today. On May 25, 2018, the GDPR became effective.[273] The GDPR is an omnibus regulation that requires businesses to protect not just consumer data but also employee PII.[274] Non-compliance results in steep fines.[275] Some have called these fines "draconian."[276]

In October of 2019, due to a so-called "configuration error," the PII of several hundred employees was leaked, due to the mishandling of cybersecurity measures by the Swedish company H&M.[277]

---

[271] *See* Wright, *supra* note 11.

[272] 6 Computer Law § 51.04 (2020) ("Since the Directive was released in 1995, it has gradually become apparent to the EU that the Directive had two deficiencies that required rectification. First, although one of the three goals of the Directive was to harmonize EU privacy law, the EU conceded it had failed to do so. Instead, in transposing the Directive, each Member State had added its own 'bells and whistles.' In addition, as time went on, the Directive gradually became obsolescent or difficult to apply as technology inexorably advanced." (footnotes omitted)).

[273] *Id.*

[274] Rebecca Hughes Parker, *H&M's $41M GDPR Fine Underscores Importance of Employee Data Handling*, CYBERSECURITY LAW REPORT (April 20, 2020), www.cslawreport.com/7703636/handms-and3641m-gdpr-fineunderscores-importance-of-employee-data-handling.thtml.

[275] Michael Nadeau, *General Data Protection Regulation (GDPR): What you need to know to stay compliant*, CSO (June 12, 2020), www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.

[276] *See* 6 Computer Law § 51.04 ("The inclusion of draconian maximum fines in the GDPR is designed to encourage enterprises to comply, in contrast to the benign neglect that characterized the approach of many enterprises to the Directive.").

[277] Press Release, The Hamburg Comm'r for Data Prot. and Freedom of Info., 35.3 Million Euro Fine for Data Protection Violations in H&M's Service Center (Oct. 1, 2020), cdn.wide-area.com/acuris/files/cybersecurity-law-report/legalmaterials/2020-10-01-press-release-h%2Bm-fine.pdf [hereinafter $35.3 Million Fine].

The Hamburg Commissioner for Data Protection and Freedom of Information explained in a press release that since at least 2014, at H&M's Hamburg office, "parts

The leak happened due to recorded conversations with employees and the human resources managers when employees returned from vacation.[278] The recordings sometimes had sensitive employee information, such as health issues and details from their private lives.[279] Hamburg's Data Protection Authority "levied Germany's largest GDPR fine so far," €35.3 million (about $41.4 million), as a result of the breach.[280] Dominik Weiss, partner at Hamburg branch office of law firm Bryan Cave Leighton Paisner, remarked that "this case … illustrates how initially small-scale data collection and processing activities, which may have been carried out in compliance with applicable data protection laws, can grow, without the relevant privacy structure and processes in place, into processing activities that significantly breach the GDPR's principles."[281] The company not only had to pay the fine, but also plans on paying the employees a considerable compensation.[282] Hamburg's Commissioner for Data Protection and Freedom of Information said the fine was "adequate and effective to deter companies from violating the privacy of their employees."[283]

VII. A NEED FOR COMPANIES TO HEIGHTEN THE PROTECTION OF EMPLOYEE PERSONAL IDENTIFICATION INFORMATION

The United States economy relies on consumers to trust in certain brand and spend money. If a consumer fears that a website is unsafe, she will shop elsewhere and not risk her credit card data. But when a person gets a job, she will often have to submit copies of photo identification cards which contain not only a facial image but also an address, along with a background check and credit report, bank account information for payroll, and sometimes fingerprints. This is very valuable information to a cybercriminal; employee PII is more attractive to hackers than consumer credit card data.[284] Half of the Circuits hold that a future risk is too remote for standing in data

---

of the workforce have been subject to extensive recording of details about their private lives." *Id.* at 1.

[278] *Id.*

[279] *Id.*

[280] *See* Parker, *supra* note 276.

[281] *See id.*

[282] $35.3 Million Fine, *supra* note 279.

[283] *Id.* at 2.

[284] *See* Sharma, *supra* note 15.

breach cases,[285] which includes not only consumer data but also employee PII. Thus, today's legal system offers limited recourse to employees who are victims of a data breach. An employee cannot sue the overseas hackers who committed the cybercrime,[286] and an employee has no standing to sue the employer where the breach occurred in half of the United States Circuits. This is compounded by the lack of federal regulation over the private sector's treatment of employee PII.

In contrast to GDPR regulation, which mandates taking steps to safeguard employee PII, the United States has an aspirational model, that suggests steps for companies to take. If cybersecurity litigation does arise, the only legal standard companies must show is the "reasonably prudent cybersecurity measure."[287] This is an undefined standard which provides only basic, non-mandatory guidance to companies.[288]

The Supreme Court, based on the holdings in *Ashcroft, Twombly*, and *Clapper*, maintains that a future risk is not enough to confer standing. It is extremely difficult to trace where data goes on the dark web.[289] Added to the lack of standing to even bring suit in data breach cases, there is little incentive to companies to invest beyond basic cybersecurity standards.

The question therefore remains as to how to best protect sensitive employee PII in the United States when corporations are not under threat of a lawsuit, due to lack of standing, nor a fine, due to lack of federal regulation. An omnibus federal cybersecurity regulation like the GDPR may be a logical next step, but it could also be punitive for corporations.[290] It is arguable that steeper fines akin to that of the GDPR would encourage companies to protect employee data in the U.S., but if a company already has reasonably prudent cy-

---

[285] *See supra* Part IV.

[286] *See* FBI, *supra* note 14.

[287] *See* Smedinghoff, *supra* note 73 ("Corporate legal obligations to implement security measures are set forth in an ever-expanding patchwork of generally applicable state, federal, and international laws, regulations, and enforcement actions, as well as common law duties and other express and implied obligations to provide 'reasonable' or 'appropriate' security for corporate data. And these obligations apply to both regulated and non-regulated industries.").

[288] *Id.*

[289] *See* After the Breach, What Happens to Your Data?, *supra* note 20.

[290] *See* Parker, *supra* note 276. H&M was fined $41M under GDPR in October 2020 for breach involving employee PII. *Id.*

bersecurity program in place, a steep fine could hurt a business more than help employees whose data were hacked.

As it stands now, the United States will likely continue to see litigation arise on a case-by-case basis when employee PII is the subject of a data breach. The problem for employees is that they will likely not have standing to bring suit in the first place, and there is no way to determine if their data are being misused on the dark web.[291] And, it is arguably unfair to punish a company for a breach when the real criminal is a hacker. Thus, employee data remains vulnerable under the current standards, and the onus is on companies to self-regulate to ensure they do right by their employees.

[291] *See* After the Breach, What Happens to Your Data?, *supra* note 20.