Bridging the Gap:

How the Injury Requirement in FTC Enforcement Actions and Article III Standing are Merging in

The Data Breach Realm

By Amy Grewal Dunn*

The company's computer network is then attacked and someone gains unauthorized access to the company's servers and becomes privy to your personal information.

Introduction

The story has become all too familiar in recent headlines: you use your credit or debit card at a store and provide a company with your personal information, such as your social security number, address, and phone number. The company's computer network is then attacked and someone gains unauthorized access to the company's servers and becomes privy to your personal information. The company learns of this data breach and, as required by law, notifies you of the breach. You take steps to secure your information: You cancel your cards, purchase credit-monitoring services and consider buying identity theft insurance. This stolen information is then used against you, and you spend considerable time and money to contravene the effects of the breach. You worry you have become a victim of identity theft.

In most cases, federal law protects you against financial loss or the company will reimburse you for the fraudulent charges. But what about the mitigating expenses you incurred to protect your identity? Or what if your information is stolen, but not necessarily misused right away–do you wait, not knowing if it will be next week, next month, or next year? And can you be compensated for the many hours it took to take all the necessary protections?

Technology advances everyday at a speed in which consumers and businesses are unfortunately unable to keep up. Each year, more and more companies collect personal information from consumers–including social security numbers and credit and debit card numbers–and with that comes a rise in the amount of data breaches occurring each year.[2] Thus, it is of no surprise that companies' data security practices have come under scrutiny. Target, Sony, Ashley Madison, Anthem and Home Depot are just a few of the companies that have dominated headlines in recent years for their data breaches.[3] Although 2014 is fondly referred to as "the year of the breach," 2015 managed to double the number of breached records in just eight months.[4] Seven out of ten organizations worldwide in 2015 were victims of successful data breaches.[5] Between 2005 and December 31, 2015, the Identity Theft Resource Center estimates 5,810 data breaches occurred with more than 840 million records compromised.[6] Who holds these companies accountable for their lax security protection?

The Third Circuit recently released its much-anticipated opinion in *FTC v. Wyndham Worldwide Corp.*, affirming the United States District Court for the District of New Jersey's decision.[7] This decision is a game changer for the data privacy and security industry, as it establishes the Federal Trade Commission's (FTC) authority to regulate privacy and data security.[8] Specifically, this decision allows the FTC to challenge an entity's data security practices under the unfairness test of section 5 of the FTC Act.[9] The FTC contends the harm that resulted from Wyndham's conduct was sufficient to constitute substantial injury.[10] An FTC Opinion by the Commission in *In Re LabMD* may further embolden the FTC's power to regulate online data privacy under the unfairness test.[11] Although there was no evidence of actual consumer injury, the Commissioners found that disclosure of personal information, including medical records, constituted a substantial injury.[12]

On the other side of the playing field in the data breach realm are private and class action lawsuits. The Seventh Circuit's decision in *Remijas v. Neiman Marcus* has made it easier for consumers to move forward with data breach class-action lawsuits by holding that future harm, such as resolving fraudulent charges and protecting oneself against future identity theft, are injuries sufficient to survive a motion to dismiss under Article III Standing.[13] This holding reverses the District Court for the Northern District of Illinois' decision,[14] which was relied on by Wyndham in its reply brief to the Third Circuit,[15] and supports the FTC's contention that its complaint against Wyndham sufficiently alleged consumer harm.[16] The Administrative Law Judge (ALJ) in *In Re LabMD* also relied on this case in his Initial Decision, noting that a criminal act for the purposes of committing identity theft is more persuasive in determining whether a "substantial injury" has occurred, versus situations in which *no* alleged harm has occurred.[17]

While the FTC's enforcement efforts and private litigation lawsuits are separate and distinct, several recent cases demonstrate that their respective injury requirements—specifically in the context of future harm after a data breach—is not only unsettled in the legal world, but crossing paths.

The purpose of this Note is to shed light on security practices that the FTC and courts deem inadequate in the context of online data privacy, by examining the injury threshold that the FTC and consumers must satisfy in order to bring action against a company. Despite critics' arguments that the FTC cannot or should not regulate online data privacy, *Wyndham* has cemented the FTC's role as our nation's cyber security watchdog.[18] Part I of this Note reviews how the FTC's unfairness authority has evolved since its enactment, and examines the FTC's past policy statements on unfairness to demonstrate its shift from public policy to consumer injury. Part II discusses recent FTC decisions and illustrates how the FTC's three-prong unfairness test is applied in a data breach context, with emphasis on the alleged harm. Part II also discusses and analyzes recent developments in *Wyndham* and *LabMD* to illustrate the arguments the FTC has made to allege sufficient injury against companies that have faced data breaches. Part III explores the injury-in-fact requirement under Article III Standing jurisprudence as it relates to substantial injury under the FTC's unfairness test and provides a brief overview of the data breach cases that led to the Seventh Circuit's decision in *Remijas v. Neiman Marcus*. Finally, the Note concludes by revealing common themes in recent court decisions in regards to future harm.

I. The FTC's Unfairness Authority

A. History & Development of the Unfairness Test

Understanding who the FTC is and what it does is important before exploring its role in consumer privacy regulation. The Federal Trade Commission Act (FTC Act) was enacted in 1914 to outlaw unfair methods of competition[19] by establishing the FTC, a federal agency tasked with enforcing the provisions of the FTC Act and preventing the use of unfair methods of competition.[20] The Wheeler-Lea Act of 1938 amended the FTC Act to include not only prohibition of "unfair or deceptive acts or practices," but also to protect consumers in addition to competition.[21] Between 1938 and 1964, the FTC described certain acts as both "unfair and deceptive" without specifying whether an act was "unfair" or "deceptive."[22] It was not until 1964 that the FTC first shed light on its interpretation of "unfair" by setting forth an unfairness test developed in connection

with a trade regulation rule regarding the advertising and sale of cigarettes.[23] This test, known as the "Cigarette Rule,"[24] provides three factors for determining whether an act or practice is "unfair":

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise-whether, in other words, it is within at least the penumbra of some common- law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; (3) whether it causes substantial injury to consumers (or competitors or other businessmen).[25]

In 1972, the Supreme Court cited to the "Cigarette Rule" unfairness criteria in a footnote in *FTC v. Sperry & Hutchinson*.[26] Whether the Supreme Court explicitly approved the criteria has been a matter of debate,[27] but the *Sperry* decision nevertheless legitimized the unfairness test and the FTC began a "series of rulemakings relying upon broad, newly found theories of unfairness."[28] However, the FTC struggled with applying the "Cigarette Rule" factors consistently, and in its attempt to attack companies for unethical or immoral behavior, earned the nickname "National Nanny." Concerned, Congress withheld funding from the FTC and enacted legislation to preclude the FTC from using unfairness to ban certain advertisements.[29] This resulted in a limitation of the FTC's use of its unfairness authority in rulemaking actions.[30]

B. Policy Statements & Shift from Public Policy to Consumer Injury

In the late 70s to early 80s, the FTC began to shift away from public policy toward consumer injury.[31] It articulated its unfairness jurisdiction in connection with the 1979 promulgation of a rule in the home insulation industry: sellers had failed to disclose certain information, which caused substantial injury to consumers by impeding their ability to make informed purchasing decisions.[32] Because of Congress' concern that the FTC's power was too broad to regulate "unfair" commercial practices, a unanimous FTC responded with its first policy statement addressing the FTC's unfairness power.[33] Using the "Cigarette Rule" criteria as a starting point, the Unfairness Policy Statement emphasized consumer injury as the most important element of the criteria, rejected the "unethical or unscrupulous standard prong, and seemed to limit the role of public policy."[34] To determine whether a practice unfairly injures consumers, the FTC adopted three factors: (1) the injury must be substantial, (2) the injury must not be outweighed by countervailing benefits to consumers, and (3) it must be an injury that consumers could have reasonably avoided.[35] Apparently chastened by its previous use of the unfairness doctrine, the FTC applied this test sparingly to situations involving consumer injury where a deception analysis would not be appropriate.[36] In 1994, Congress codified the three-part unfairness test in 15 U.S.C. § 45(n) and indicated that the role of public policy was limited; although the FTC could consider public policy, it could not find unfairness on an independent basis of public policy alone.[37] Despite the codification of the Unfairness Policy Statement, the FTC continued to assert its unfairness authority in limited circumstances.[38] It was not until the late 1990s, with the rise of the Internet, that data security became a prevalent issue.[39]

C. Settlements & Consent Orders

The FTC's authority includes two separate authorities: investigative authority and enforcement authority.[40] After an investigation has been conducted, the FTC may exercise its enforcement authority through an administrative or judicial process:

> When there is "reason to believe" that a law violation has occurred, the Commission may issue a complaint setting forth its charges. If the respondent elects to settle the charges, it may sign a consent agreement (without admitting liability), consenting to entry of a final order, and waive all right to judicial review. If the Commission accepts such a proposed consent agreement, it places the order on the record for thirty days of public comment (or for such other period as the Commission may specify) before determining whether to make the order final.[41]

The majority of actions enforced by the FTC result in consent orders, which allow companies "to avoid admitting wrongdoing in exchange for remedial measures" and result in settlements.[42] The FTC relies on these settlements and consent letters to inform companies of the rules it wants them to follow.[43] According to privacy law expert Daniel Solove, these settlements essentially function as common law because the FTC's settlements usually contain complaints and consent orders, and are published on the FTC's website.[44] In addition to their publication, the FTC's settlements "serve as a useful way to predict future FTC activity."[45]

Although the FTC has issued almost two-hundred privacy-related complaints against companies, many of them have settled.[46] And as of last year, the FTC has settled more than twenty cases in which companies' failures to reasonably protect consumer data constituted unfair practices.[47] Only two cases, *FTC v. Accusearch Inc.,*[48] and *FTC v. Wyndham*, have resulted in judicial opinions, and *In re LabMD* was recently decided by an FTC Administrative Law Judge.[49]

II. Applying the FTC's Unfairness Test to Data Breaches & Online Privacy

A. The FTC's Report to Congress

In 1999, the FTC was optimistic that self-regulation was the solution to online consumer protection and privacy.[50] Only a year later, the FTC retreated from this position and indicated it would adhere to a new policy in which it would "expand enforcement of existing laws" instead of attempting to enact legislation.[51] As part of this new policy, the FTC would utilize its unfairness test to hold organizations accountable in the event of a data breach.[52]

To further the goals of its new policy and in response to the growth of the internet marketplace–more specifically, the online consumer marketplace–the FTC issued a report to Congress detailing its recommendations for ensuring and protecting consumer privacy.[53] Among its recommendations were that Congress enact legislation directing all consumer-related Internet sites that collect personal information to comply with four practices: (1) *notice*, which mandates all Internet sites to inform consumers of their information protocol, including the information collected, how it is collected, and how it is used; (2) *choice*, in which sites would provide consumers with options as to how their information is used other than the intention for which it was obtained; (3) *access*, where sites must give consumers "reasonable" access to the information they have collected; and (4) *security*, in which sites would be required to protect consumer information in a "reasonable" manner.[54] With its new policy and initiatives, the FTC "delved into the data-security breach realm, heralding a new era of consumer protection and organizational accountability."[55]

B. Preliminary Cases

1. BJ's Wholesale Club, Inc.

BJ's Wholesale Club marks the first time the FTC solely utilized its unfairness arm without alleging "deceptive" practices in the realm of privacy and data security regulation.[56] BJ's is a nationwide membership store whose members often use credit or debit cards to purchase items.[57] BJ's collected members' personal information via wireless scanners in order to secure approval for these credit card and debit card payments.[58] In late 2003 and early 2004, banks found fraudulent charges that were made using counterfeit copies of debit and credit cards.[59] The same information that BJ's collected and put on its computer network was on these counterfeit cards.[60] In its complaint, the FTC alleged that between November 2003 and February 2004, BJ's did not "employ reasonable and appropriate measures to secure information collected at its stores" and these actions constituted an unfair practice in violation of Section 5(a) of the FTC Act.[61] Specifically, the complaint made the following allegations against BJ's, stating it:

> (1) did not encrypt the information while in transit or when stored on the in-store computer networks;
> (2) stored the information in files that could be accessed anonymously -- that is, using a commonly known default user id and password;
> (3) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks;
> (4) failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and
> (5) created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, and in violation of bank rules.
> As a result, a hacker could have used the wireless access points on an in-store computer network to connect to the network and, without authorization, access personal information on the network.[62]

Although neither the FTC's Complaint nor Decision and Order stated whether one or all violations constituted an "unfair" practice, it appears that BJ's engaged in a number of practices that from the FTC's viewpoint, amounted to unreasonable security measures for sensitive personal information. As a result of this breach–the fraudulent transactions allegedly totaled $13 million[63]–customers and banks were forced to cancel and re-issue thousands of credit and debit cards. Consumers could not use their cards to access credit and bank accounts in the interim.[64] Being that this case was the first time the FTC sought to apply its unfairness authority without asserting a deceptive practice, this case essentially provided the FTC with an important stepping stone in the realm of data privacy. It demonstrated that in the eyes of the FTC, lack of information security constitutes an unfair practice.

2. DSW, Inc.

Less than four months after the FTC issued its decision in *BJ's*, the FTC announced DSW had agreed to settle charges brought against them for their failure to take reasonable measures to protect consumer data.[65] DSW is a nationwide shoe store and similarly to BJ's, collected information from consumers for credit card, debit card, and check purchases at its stores.[66] The information collected was stored in computer networks in-store and on corporate computer networks.[67] In March 2005, DSW released a press release informing consumers that credit card and purchase information had been stolen.[68] A month later, DSW issued another press release detailing the specific locations affected by the breach and informing customers that checking account and driver's license information had also been stolen.[69] The FTC alleged in its complaint that until March 2005, DSW engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information collected at its stores. Specifically, that DSW:

> (1) created unnecessary risks to the information by storing it in multiple files when it no longer had a business need to keep the information;
> (2) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks;
> (3) stored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password;
> (4) did not limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and
> (5) failed to employ sufficient measures to detect unauthorized access. As a result, a hacker could use the wireless access points on one in-store computer network to connect to, and access personal information on, the other in-store and corporate networks.[70]

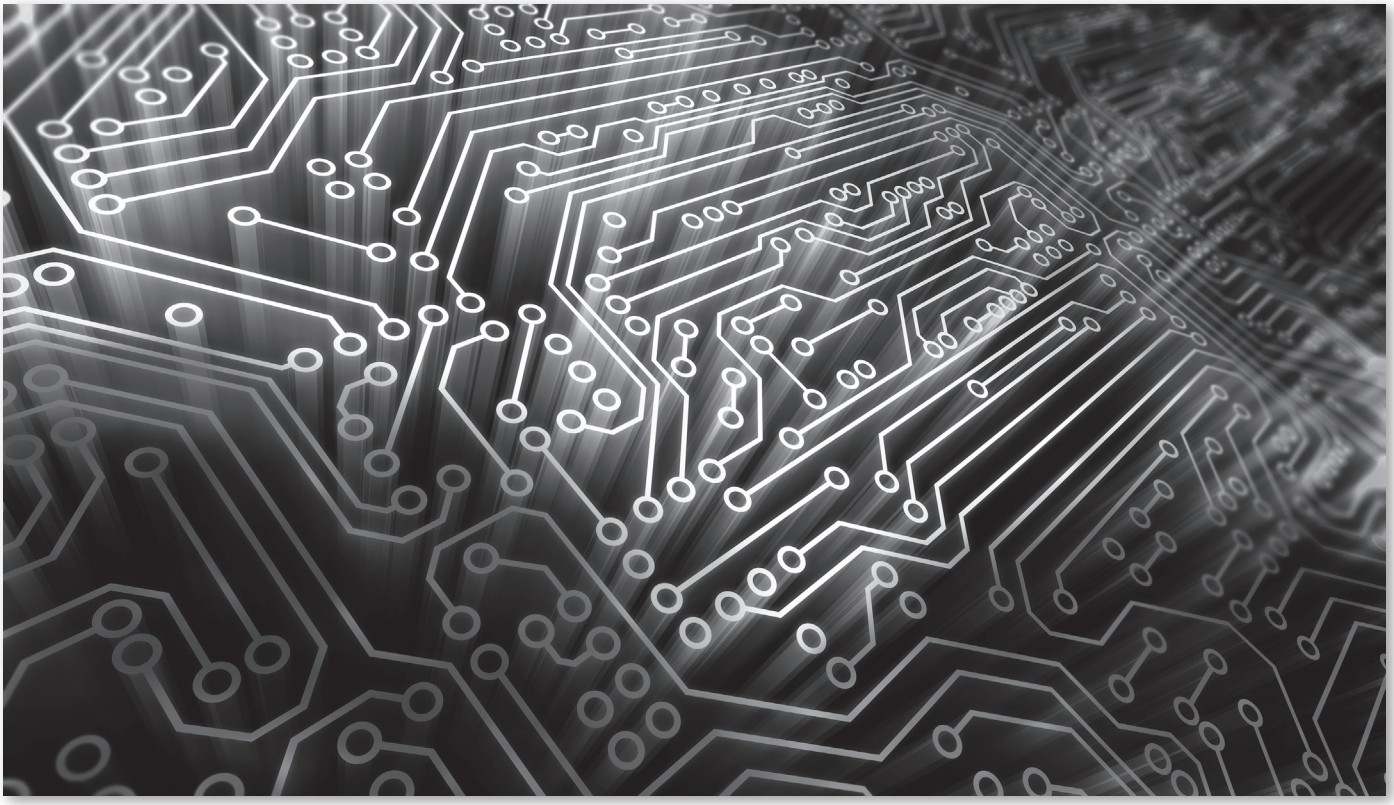
More than 1.4 million credit and debit cards were compromised, as well as 96,385 checking accounts and driver's license numbers.[71] At the time of FTC's complaint, fraudulent charges had already been discovered on some of the accounts.[72] Many customers were advised to close their accounts, and in doing so, not only lost access to those accounts, but incurred expenses.[73]

3. Dave & Buster's, Inc.

Dave & Buster's is yet another case in which sensitive consumer data was stored in the company's network.[74] For a period of four months, someone hacked into Dave & Buster's network, installed software, and obtained personal information while it was in transit from its in-store networks to their credit card processing company.[75] Upon learning of the breach, Dave & Buster's sent notifications to law enforcement and the consumers' credit card companies.[76] By the time FTC issued its complaint, however, banks had collectively claimed several hundred thousand dollars in fraudulent charges.[77] Roughly 130,000 consumer cards were compromised, and as in the cases of *BJ's Wholesale Club* and *DSW*, the FTC utilized its standard go-to language: "Respondent's failure to employ reasonable and appropriate security measures to protect information caused or is likely to cause substantial injury to consumers…"[78]

C. Substantial Injury & Recent Developments in Data Privacy

As noted earlier, the FTC considers consumer injury to be the primary focus of the FTC Act and the most important "Cigarette Rule" criteria.[79] Depending on the circumstances, consumer injury alone is sufficient to render a practice "unfair."[80] An act is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[81] The primary focus of the remainder of this Note will address the substantial injury requirement, as outlined in 15 U.S.C. § 45(n). In determining what constitutes "substantial injury," the FTC's 1980 Policy Statement is a good starting point. It provides:



> The Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction. Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair. Thus, for example, the Commission will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers, as has been suggested in some of the comments.[82]

The Consumer Financial Protection Bureau further supplements the FTC's definition of substantial injury and provides examples of both monetary harm and non-monetary harm:

> Monetary harm includes, for example, costs or fees paid by consumers as a result of an unfair practice. An act or practice that causes a small amount of harm to a large number of people may be deemed to cause substantial injury.
>
> Actual injury is not required in every case. A significant risk of concrete harm is also sufficient. However, trivial or merely speculative harms are typically insufficient for a finding of substantial injury. Emotional impact and other more subjective types of harm also will not ordinarily amount to substantial injury. Nevertheless, in certain circumstances, such as unreasonable debt collection harassment, emotional impacts may amount to or contribute to substantial injury.[83]

1. FTC v. Wyndham Worldwide Corp.

Wyndham Worldwide Corporation ("Wyndham") was the first entity to challenge the FTC's authority to regulate lax data security practices under its unfairness test.[84] The FTC sued Wyndham in 2012 in federal district court, alleging Wyndham "failed to employ and appropriate measures to protect information against unauthorized access," thus violating Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).[85] As a result of these failures, Wyndham suffered from three data breaches between 2008 and 2009.[86] Hackers used similar methods during each breach to access personal consumer information on Wyndham's hotel servers.[87] The FTC provided a list of at least ten ways in which Wyndham failed to provide reasonable security and stated that Wyndham "engaged in unfair cyber security practices that, 'taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.'"[88] More than 619,000 account numbers were compromised and fraud loss totaled over $10.6 million.[89] "Consumers and businesses suffered financial injury, including but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit . . . Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm."[90] The FTC's Complaint alluded to the fact that not only had consumers already suffered harm, but they would also *continue to suffer substantial injury*.[91]

At Wyndham's request, the case was transferred to the U.S. District Court for the District of New Jersey,[92] which found that the FTC had sufficiently plead "substantial injury" to consumers caused by Wyndham.[93] Wyndham argued the FTC had not plead sufficient facts to state a claim of "substantial injury" to consumers and alleged the FTC had made conclusory statements without identifying specific consumers who suffered specific financial injury as a result of the criminal cybersecurity attacks on Wyndham.[94] Such preciseness and exactness, Judge Salas countered, is "essentially an appeal for a heightened pleading standard."[95] The court commented on Wyndham's lack of authority for this assertion, but declined to impose a heightened pleading

The FTC stated Reilly concerned Article III Standing and differentiated between particularized injury that is "actual" and "imminent," and practices that "cause or are likely to cause" substantial injury to any class of consumers.

standard.[96] In a footnote recognizing the dispute over whether non-monetary injuries are cognizable under Section 5, the court seemed amenable to recognizing non-monetary harm: "Although the court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act, the Court need not reach this issue given the analysis of the substantial harm element above."[97] The court denied Wyndham's motion to dismiss,[98] finding the FTC's allegations allowed the court to reasonably infer that Wyndham's "data security practices caused theft of personal data, which ultimately caused substantial injury to consumers."[99]

The Third Circuit granted Wyndham's appeal.[100] In its opening brief, Wyndham again argued the FTC's conclusory arguments failed to plead sufficient facts to state a claim of "substantial injury" as a result of the criminal cybersecurity attacks on Wyndham. [101] Interestingly, Wyndham argued "as a threshold matter," exposure of consumers' payment information and consumer efforts to remedy such exposure "do not even give rise to an injury sufficient to support Article III Standing."[102] In support of this assertion, Wyndham cited to the Third Circuit's decision in *Reilly v. Ceridian Corp*[103] and the U.S. District Court for the Northern District of Illinois' decision in *Remijas v. Neiman Marcus*.[104] The FTC countered that Wyndham's reliance on *Reilly* was misplaced for two reasons.[105] First, there was no evidence in *Reilly* that data was acquired or misused; instead, the injury rested on speculation that the hacker had obtained information and intended to commit future fraud.[106] Here, the FTC stated, its complaint against Wyndham alleged actual theft and actual misuse of data.[107] Regarding misuse of data, the FTC pointed to two cases to support its assertion that time, expense, and effort to remedy injuries constitutes substantial injury.[108] Second, the FTC stated *Reilly* concerned Article III Standing and differentiated between particularized injury that is "actual" and "imminent," and practices that "cause or are likely to cause" substantial injury to any class of consumers. The Third Circuit ultimately affirmed the district court and held that a company's alleged failure to maintain reasonable and appropriate data security, if proven, *could* constitute an unfair method of competition in commerce.[109] A few months later, Wyndham and the FTC entered into a settlement, in which Wyndham agreed to establish a comprehensive information security program, designed to protect cardholder data, and perform annual security audits to ensure compliance with the program.[110]

2. In Re LabMD, Inc.

LabMD is the first of two organizations, along with Wyndham, to challenge the FTC's authority over data security practices.[111] The FTC began investigating medical testing laboratory LabMD in 2010[112] after learning that personal consumer information LabMD had collected, including medical data, was allegedly available to the public on a peer-to-peer ("P2P") file-sharing network.[113] The FTC then filed an administrative complaint against LabMD in August 2013, alleging it had failed to reasonably protect consumer information, including medical data, which caused or would be likely to cause substantial injury.[114] Thus, LabMD had engaged in an unfair practice and violated Section 5(a) of the FTC Act and 15 U.S.C. §45.[115] Instead of settling, as most companies do, LabMD filed a motion to dismiss.[116]

What began as an enforcement effort on behalf of the FTC evolved into an arduous six-year administrative battle that resulted in multiple lawsuits[117] and the demise of LabMD.[118] Accordingly, background is necessary to flesh out some of the key issues in this case. In 2008, Tiversa, a data security company offering data breach remediation services, contacted and notified LabMD that a file containing LabMD's consumers' personal information had been discovered on a P2P network.[119] In its investigation, LabMD determined that LimeWire–a P2P file-sharing application–had been downloaded and installed on one billing computer, removed LimeWire from that computer, and made efforts to search P2P networks for the file.[120] Tiversa tried to sell its services to LabMD, representing that the file had spread across P2P networks.[121] In what appears to be retaliation and ill motives,[122] Tiversa employees turned over the file to the FTC in hopes that fear of an enforcement action would compel LabMD to purchase Tiversa's services.[123] Documents and deposition testimony from Tiversa formed the basis for one of two incidents in the FTC's complaint,[124] and were relied upon by the FTC's expert witnesses to determine the likelihood of identity theft harm.[125] By the time Tiversa's credibility came to light, the discovery period was long gone and the FTC and LabMD were mid-trial.[126] FTC Chief Administrative Law Judge Michael Chappell dismissed the FTC's complaint against LabMD[127]:

> Complaint Counsel has failed to carry its burden of proving its theory that Respondent's alleged failure to employ reasonable data security constitutes an unfair trade practice because Complaint Counsel has failed to prove the first prong of the three-part test – that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers.[128]

Without specifically addressing whether LabMD's security practices were in fact "unreasonable," Judge Chappell found there was no evidence that the limited exposure of the file discussed above caused, or would be likely to cause, harm to consumers. Further, the court rejected the FTC's assertions that emotional harm, such as embarrassment, would be likely to occur and that such emotional harm would even constitute substantial injury.[129] "At best, Complaint Counsel have proven the possibility of harm, but not any 'probability or likelihood of harm.'"[130]

Important, however, was Judge Chappell's analysis of an FTC Section 5 unfairness claim and the "substantially injury" prong. He began his analysis of "unfair" conduct by trudging through the history and development of the "unfairness" test and defining "identity theft harm."[131] He then provided a list of the FTC's allegations constituting "substantial injury":

- Likely identity theft harm for consumers whose Personal Information was exposed in the 1718 File and the Sacramento Documents, including monetary losses from NAF, ECF, and ENCF, based on an "increased

risk" that consumers whose information is exposed in a data breach will suffer identity theft harm;
- Likely medical identity theft harm for consumers whose Personal Information was exposed in the 1718 File, including monetary losses due to fraudulently procured medical products and services, and health and safety risks;
- "Significant risk" of reputational harm, privacy harm, and/or other harms based on stigma or embarrassment, caused by the unauthorized exposure of asserted "sensitive medical information" in the 1718 File; and,
- "Risk" of harm to all consumers whose information is maintained on LabMD's computer network, which Complaint Counsel variously describes as the "risk," "increased risk," or "significant risk," that Respondent's computer network will suffer a future data breach, resulting in identity theft harm, medical identity theft harm, and/or other harm.[132]

In response to LabMD's argument that no consumer had suffered actual harm, the FTC argued proof of likely harm is sufficient in an unfairness analysis.[133] The ALJ noted the fact that many years had passed by without any indication that any consumer had suffered harm as a result of LabMD's data security practices "undermines the persuasiveness" of the FTC's assertion that harm is "likely" to occur.[134] To hold LabMD liable for unfair practices without proof of actual injury to *any* consumer would "require speculation and would vitiate the statutory requirement of 'likely' substantial consumer injury."[135] The ALJ then cited to several cases to support its theory that historically, actual harm–not "likely" harm–has resulted in liability for unfair practices.[136] Noting that Section 5(n) of the FTC Act does not define the word "likely," he combined case law and dictionary definitions to conclude "likely" means "probable," not "possible." The ALJ also rejected the FTC's argument that the "significant risk" language from the FTC's 1980 Unfairness Policy Statement meets the "likely" requirement, finding Congress's omission of "significant risk" in its Senate Report demonstrates Congress rejected that standard.[137]

In July 2016, the FTC reversed the ALJ's Initial Decision and issued and Opinion and Final Order against LabMD, concluding that the ALJ applied an incorrect legal standard and finding LabMD's security practices to be "unfair" and unreasonable.[138] Specifically, FTC Chairwoman Edith Ramirez stated that the exposure of the file containing LabMD's consumers' personal information not only caused substantial injury, but was was also likely to cause substantial injury.[139] As to the first point, the Commissioners noted that because LabMD failed to notify the customers whose information was disclosed, there is no way to know if the breach of the file resulted in any type of identity theft.[140] However, the Commissioners found that the *disclosure* of medical information itself constituted a "substantial injury" because it caused non-economic harm such as embarrassment and reputation harm.[141] In emphasizing that disclosure of sensitive medical information harms consumers, the Commissioners turned to federal and state cases, tort law, and federal regulations such as HIPPA and the Fair Credit Reporting Act.[142]

The Commissioners also found that a showing of "significant risk" adequately meets the "likely to cause substantial injury" standard.[143] Addressing the ALJ's arguments in turn, the Commissioners disagreed with the ALJ's interpretation and meaning of "likely," noting that different dictionaries use various definitions.[144] In addition, the Commissioners stated there was no evidence in the legislative history of Section 5(n) to indicate that Congress intended to reject "risk of harm" as a substantial injury.[145] In regards to harm, the opinion emphasized that compromised medical records in data breach cases can effect a consumer's health or safety as a result of misdiagnoses or mistreatment of illness.[146] Both the significant risk of harm and "high likelihood of a large harm," the Commissioners concluded, demonstrated that the exposure of the file constituted substantial injury: "We need not wait for consumers to suffer known harm at the hands of identity thieves."[147]

As Judge Chappell recognized in his Initial Decision, this case presented a low risk of identity theft harm, compared to cases like *Wyndham* and *Neiman Marcus*, where stolen personal information was used to commit credit card fraud. Whereas here, it did not appear to be the case that Tiversa downloaded a file in an effort to make fraudulent charges on consumers' credit cards. While Judge Chappell did not entirely foreclose the notion that future harm cannot constitute a "substantial injury," the Commissioners' opinion seems to echo the Seventh Circuit's view in *Remijas v. Neiman Marcus*, discussed below.

III. Private Lawsuits & Class Action Lawsuits

Going back to the hypothetical at the beginning of this Note, there is another recourse available to individuals who have been victims of a data breach: litigation, in the form of either a private lawsuit or class action suit. Claims brought by individuals in response to data breaches often stem from state tort or contract law, such as negligence or breach of implied contract.[148] Both claims "require that the plaintiff be damaged in some cognizable way."[149]

A. Article III Standing and the "Injury-in-Fact" Requirement

The biggest obstacle plaintiffs in data breach cases face is whether their injury is even something the law recognizes.[150] Article III of the United States Constitution permits courts to hear a "case" or "controversy" only if a plaintiff has "standing" to sue.[151] Under this "standing" doctrine, a party can sue another party if the following three constitutional requirements are met: (1) *injury-in-fact*, in which the plaintiff must show the harm is "concrete and particularized," and "actual or imminent"; (2) *causation*, in which the injury must be traceable to the defendant's conduct; and (3) *redressability*, meaning it must be likely–and not speculative–that a favorable decision will redress the injury.[152] Defendants in data breach cases often challenge a plaintiff's standing by motioning to dismiss[153] and courts must dismiss these cases if the plaintiff fails to establish standing by meeting these three requirements.[154] This Note further explores the injury-in-fact element.

Claims brought by individuals in response to data breaches often stem from state tort or contract law, such as negligence or breach of implied contract.

If a plaintiff's personal information *has* been stolen and is used to make purchases, then establishing the injury-in-fact requirement is fairly straightforward because the plaintiff has been directly harmed.[155] These plaintiffs usually seek damages for what are considered to be cognizable injuries–unauthorized purchases and damaged credit scores.[156] However, plaintiffs whose stolen information was not used to incur charges face an uphill battle in establishing standing.[157] In such instances, these plaintiffs usually claim they have been harmed by having to spend money on credit monitoring services, identity theft insurance, and replacement cards and checks; in addition, they may seek damages for the increased risk of future injury and emotional distress.[158] Whether this indirect harm constitutes injury-in-fact without a showing of actual damages has been the subject matter of many debates,[159] and courts are currently split on the issue.[160] Case law to date is replete with inconsistencies regarding a plaintiff's right to sue when his or her information has been illegally obtained, but not used for fraudulent purposes.[161] However, the consensus among courts now sways in favor of dismissing such cases for lack of an injury-in-fact.[162]

B. Recent Developments

1. Pre-*Clapper* Circuit Split

As cybersecurity law evolved in the 2000s, the issue of standing in data breach cases led to differing outcomes among lower district courts, and ultimately, a circuit split among the Third, Seventh, and Ninth Circuits.[163] In 2007, the Seventh Circuit seemed to adopt a more liberal view of standing in data breach cases as opposed to some of the lower districts and held in *Pisciotta v. Old National Bancorp* that a risk of future harm was sufficient to satisfy Article III standing's injury-in-fact requirement.[164] The plaintiffs in *Pisciotta* sued their bank after a hacker accessed personal information through the bank's website and sought compensation for the purchase of credit monitoring services.[165] Three years later, the Ninth Circuit reached the same conclusion in *Krottner v. Starbucks Corp*, finding a "credible threat of harm" that is "both real and immediate, not conjectural or hypothetical" conferred standing.[166] In *Krottner,* Starbucks employees sued their employer after a laptop was stolen containing unencrypted employee data.[167] If the laptop had not been stolen, the court stipulated, and the employees had sued under the theory that it would be at some point be stolen in the future, the threat of harm would be "far less credible."[168]

In 2011, the Third Circuit diverged from its sister courts and held an allegation of future harm in data breaches was too speculative and neither "imminent" nor "certainly impending" to warrant standing.[169] In *Reilly v. Ceridian Corp.,* employees of a law firm sued Ceridian, a payroll-processing firm, after Ceridian discovered a hacker may have penetrated its firewall and accessed more than 20,000 employees' personal and financial information.[170] Although "whether the hacker read, copied, or understood the data" was unknown, Ceridian offered to provide credit monitoring services and identity theft protection to individuals whose information was potentially stolen.[171] The plaintiffs' allegations included increased risk of identity harm, costs incurred to monitor credit activity, and emotional distress.[172] The court dismissed the case for lack of standing and placed particular emphasis on the fact that the plaintiffs' injuries could not be described without the word "if": "*if* the hacker read, copied and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will [plaintiffs] have suffered an injury."[173] The court found *Pisciotta* and *Krottner* to be of little persuasive value: in *Pisciotta*, the hacker's conduct was "sophisticated, intentional, and malicious" and in *Krottner*, there was evidence of misuse of a plaintiff's personal information.[174]

2. *Clapper v. Amnesty International*

In 2013, the Supreme Court issued its first opinion on standing since the emergence of privacy and data breach cases.[175] In *Clapper v. Amnesty International*, respondents—an individual and several organizations—challenged the constitutionality of the Federal Intelligence Surveillance Act, which authorizes government officials to put individuals under surveillance and intercept foreign communications.[176] The respondents alleged they had satisfied the injury-in-fact requirement under the standing doctrine based on two theories: (1) *future injury*, in which there was an "objectively reasonable likelihood" that confidential information would be intercepted at some point, and (2) the costs and measures expended to protect the confidentiality of their communications from surveillance constituted *present injury*.[177] In addressing these two theories, respectively, the Supreme Court found that the respondents' arguments were based on "a speculative chain of possibilities that [do] not establish that their injury is certainly impending"[178] and fear that caused respondents to incur costs.[179] In a 5-4 decision, the Supreme Court held that the respondents had failed to satisfy the injury-in-fact threshold because respondents had not demonstrated that an "imminent ham" was present[180] or shown that the threatened injury was "certainly impending."[181]

In his dissent, Justice Breyer emphasized that "certainly impending" is a "somewhat elastic concept" that is not to be read literally or refer to absolute certainty,[182] and that the Supreme Court has found standing in cases involving injury that was "far less certain than here."[183] "What the Constitution requires is something more akin to 'reasonable probability' or 'high probability.'"[184]

Despite the fact that *Clapper* did not arise within a data breach context, courts have since turned to the decision to assess whether parties have satisfied standing and it has had a significant impact in data breach cases.[185] Whether *Clapper* has overruled *Pisciotta* and *Krottner* has been the subject of debate,[186] and most federal district courts have found threat of future harm in data breach cases insufficient to establish standing.[187] But all is not lost for plaintiffs. As discussed below, there have been a few cases post-*Clapper* in which threat of future injury sufficiently established standing.

3. Finding a basis for standing in post-*Clapper* cases

Clapper is not the end-all and be-all of the existence of standing in data breach cases, as there have been some courts that have recognized a basis for standing in cases involving threat of future harm. For example, in *Moyer v. Michaels Stores, Inc.*, Michaels learned of "possible fraudulent activity" on credit and debit cards used at Michaels' stores.[188] The plaintiffs' claims included future identity theft, costs incurred to protect themselves from this future harm, and miscellaneous expenses resulting from bank withdrawals, fraudulent activity, and bank fees.[189] Relying on *Pisciotta*'s reasoning that an "elevated risk of identity theft is a cognizable injury-in-fact,"[190] the court found Michaels' data breach sufficiently imminent to give the plaintiffs standing.[191] In reaching this conclusion, the court distinguished *Clapper* on the basis that the imminence requirement in *Clapper* was applied in an "'especially rigorous' fashion" in a case involving "national security and constitutional issues."[192]

Similarly, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,* is another case in which the court relied on a pre-*Clapper* case, *Krottner*, to hold that the plaintiffs had sufficiently alleged standing.[193] Although the court found both *Clapper* and *Krottner* controlling, the court emphasized "the Supreme Court's decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requiring that the harm be 'real and immediate.'"[194]

Recently, in *Spokeo v. Robins*, the Supreme Court provided additional guidance—albeit little—on the proper framework for assessing an Article III Standing injury-in-fact analysis.[2]

Neither *Krottner* nor *Clapper* require allegations that stolen information be misused, the court surmised, and thus the plaintiffs had "plausibly alleged a 'credible threat' of impending harm."[195]

The Northern District of California echoed these sentiments in *In re Adobe Sys. Privacy Litig.* and continued the trend of relying on precedent from the Ninth Circuit.[196] Finding *Krottner* to be good law, the court nevertheless also found the harm alleged sufficient to satisfy *Clapper*.[197] In *Adobe*, hackers obtained access to Adobe's servers and remained in their network for several weeks undetected, retrieving at least 38 million customers' personal information.[198] The court found several factors to distinguish the injury in *Adobe* from *Clapper*: the hackers deliberately targeted Adobe's network and spent weeks removing customer information, eliminating the need to "speculate as to whether Plaintiff's information had been stolen and what information was taken";[199] the hackers used Adobe's system to decrypt credit card numbers, indicating an intent to misuse the information;[200] and some of the stolen information had already surfaced on the Internet at the time of litigation.[201] The court further emphasized that waiting for the plaintiffs to be victims of identity theft for the sake of conferring standing contravened the "well-established principle" that an injury does not have to have taken place or be absolutely certain to occur in order to establish a finding of injury-in-fact.[202] Of the cases Adobe cited in support of its position, the court found *Galaria* to be closest in facts.[203] The court in *Galaria* had declined to find standing based on a risk of future injury, concluding that the harm was dependent upon whether the hackers would even make an attempt to misuse the stolen information.[204] The *Adobe* court declined to follow this reasoning and proceeded to posit the question, "[A]fter all, why would hackers target and steal personal customer data if not to misuse it?"[205]

In 2015, the Seventh Circuit issued its opinion in *Remijas v. Neiman Marcus, LLC*, and the decision is likely to have a significant impact on how courts address *Clapper* in the context of data breaches.[206] In 2013, hackers gained unauthorized access to Neiman Marcus' servers, potentially exposing approximately 350,000 cards.[207] Of those, 9,200 cards were discovered to have been misused.[208] Plaintiffs sued the high-end department store on behalf of the 350,000 customers for failing to take appropriate measures to protect them against a data breach.[209] The plaintiffs pointed to actual injuries: time and money incurred to resolve the fraudulent charges, and the costs associated with protecting themselves against future identity theft.[210] The plaintiffs also asserted two imminent injuries: risk of future fraudulent charges and the risk of identity theft.[211] The district court was satisfied that the possibility of future charges was "imminent," but found the plaintiffs had failed to demonstrate a "concrete" injury because none of the fraudulent charges appeared to be unreimbursed.[212] Acknowledging that 9,200 customers had alleged an injury-in-fact sufficient for Article III standing,[213] the district court remained unconvinced that all 350,000 consumers were at risk of identity theft[214] and granted defendant's motion to dismiss.[215]

On appeal, the Seventh Circuit reversed the district court's dismissal in *Remijas*, becoming the first federal appellate court post-*Clapper* to find standing in a case involving future harm.[216] Although the Seventh Circuit could have limited the class action to just the 9,200 customers whose credit cards were misused,[217] the court noted that *Clapper* does not completely preclude future injuries from satisfying Article III standing if that harm is "certainly impending"[218] nor should courts overread *Clapper.*[219] In addition, the court emphasized that *Remijas* is distinguishable from *Clapper* because here there is no need to speculate whether information was stolen or determine what was stolen.[220] Citing to *Adobe*, the Seventh Circuit contended that "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur."[221] The court determined that the plaintiffs had made a plausible inference they would suffer from a future risk of harm, emphasizing the purpose of a hack is to "sooner or later" misuse customer data.[222] The Seventh Circuit held that future harm is sufficient to survive a motion to dismiss.[223]

Recently, in *Spokeo v. Robins*, the Supreme Court provided additional guidance—albeit little—on the proper framework for assessing an Article III standing injury-in-fact analysis.[224] *Spokeo*, like *Clapper*, does not arise out of a data breach case, but addresses Article III standing in regards to proof of harm for violation of a federal statute.[225] In *Spokeo*, Thomas Robins brought a class action suit against Spokeo, Inc. under the Fair Credit Reporting Act (FCRA) for allegedly disseminating incorrect information about him.[226] Robins, at the time, was actively seeking employment.[227] He argued the information that Spokeo published made him appear overqualified, which resulted in harm to his employment prospects.[228] The district court dismissed the case, finding he had failed to properly plead an injury-in-fact sufficient to survive Article III standing.[229] The Ninth Circuit reversed, holding that a "violation of a statutory right is usually a sufficient injury to confer standing."[230] The Supreme Court, in a 6-2 decision, found that the Ninth Circuit's injury-in-fact analysis was incomplete because it failed to assess whether Robins' injury was "concrete," and remanded for further consideration.[231] Distinguishing a "particularized" injury as one that "must affect the plaintiff in a personal and individual way" and a "concrete" injury as one that "must actually exist," is "real," and "not 'abstract,'" the court emphasized that an injury must be both particularized and concrete but did not take a position on whether the Ninth Circuit ultimately reached the right result.[232] The court further noted that "concrete" injuries can be both tangible or intangible, and that a "risk of real harm" *could* satisfy this requirement.[233]

How *Spokeo* will be applied to consumers in data breach cases remains to be seen. Although it does not appear to completely bar lawsuits involving intangible injuries or those that create a "risk of harm," it does make clear that an injury must be both particularized and concrete, which may create an obstacle for plaintiffs at the pleading stage. It is evident from the cases discussed above that the law in regards to standing in data breach cases remains unsettled, and will continue to evolve.

IV. Conclusion

In light of the cases discussed above, fear of identity theft and incurring costs to protect oneself from future identity theft *may* be sufficient to establish injury in the eyes of the FTC or the courts. The FTC and plaintiffs may point to certain other factors to strengthen their argument that future harm constitutes an injury: the "sophistication" of the hacker, the extent of the exposure, types of information stolen,[234] items stolen,[235] the intent

or target of the hacker, the length of time that has passed since the breach, and whether the organizations—arguably the "victim" of the breach—from whom the information was stolen took remedial action.[236]

Thus far, FTC has been able to rely upon the "likely to cause substantial injury" clause articulated in Section 5 of the FTC Act to hold companies liable for an unfair act or practice where no actual injury occurred. *LabMD* goes further in declaring that disclosure of sensitive personal information constitutes substantial injury even if there is no economic harm and consumers are unaware their information has been compromised. While *LabMD* does not have the final word just yet,[237] companies and consumers should take heed that an increased risk of harm or emotional harm may be sufficient to establish injury in the eyes of the FTC. The Seventh Circuit has bridged the gap between the FTC's substantial injury requirement and the Article III's injury-in-fact requirement by allowing victims of data breaches to bring forth private lawsuits where future identity theft—in other words, future harm—and fraudulent charges constitute "injury." Keeping the foregoing in mind, consumers should keep apprised of developments on both sides, as it will likely have significant implications as to whether they can bring lawsuits after a data breach if no actual injury has occurred.

** J.D. Candidate, 2017, Indiana University Robert H. McKinney School of Law, Indianapolis, Indiana; B.A, 2007, University of Texas San Antonio, San Antonio, Texas.* *I would like to thank Professor James P. Nehf, Professor of Law at Indiana University Robert H. McKinney School of Law, for his guidance and advice throughout the writing of this Note.*

---

1 Wade Williamson, *Data Breaches by the Numbers*, Security Week (Aug. 31, 2015), http://www.securityweek.com/data-breaches-numbers [https://perma.cc/7UMB-5VYK].

2 *See, e.g.*, Rick Robinson, *Two Important Lessons from the Ashley Madison Breach*, Security Intelligence (October 28, 2015), https://securityintelligence.com/two-important-lessons-from-the-ashley-madison-breach/ [https://perma.cc/K8K6-HKMC]; Jonathan Stempel, *Home Depot settles consumer lawsuit over big 2014 data breach*, Reuters (March 8, 2016 12:56 PM), http://www.reuters.com/article/us-home-depot-breach-settlement-idUSKCN0WA24Z [https://perma.cc/E7CF-FVES]; Edvard Pettersson, *Sony to Pay as Much as $8 Million to Settle Data-Breach Case*, Bloomberg Business (October 20, 2015), http://www.bloomberg.com/news/articles/2015-10-20/sony-to-pay-as-much-as-8-million-to-settle-data-breach-claims [https://perma.cc/4BK5-VKXF].

3 Williamson, *supra* note 1.

4 CyberEdge Group, *2015 Cyberthreat Defense Report: North America & Europe*, http://www.novell.com/docrep/2015/03/CyberEdge_2015_CDR_Report.pdf?utm_campaign=NetIQ%20-%20GL%20-2015-cyberthreat-defense-report-TY-15393&utm_medium=email&utm_source=Eloqua (last visited Jan. 26, 2016) [https://perma.cc/ZC96-ZG6M] (up from 6 out of 10 in 2014).

5 *Data Breaches*, Identity Theft Resource Center, www.idtheftcenter.org/id-theft/data-breaches.html (last visited Jan 25 9:39 PM) [https://perma.cc/7D77-H6X4].

6 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3rd Cir. 2015).

7 *Id.*

8 *Id.* Section 5 of the FTC Act is codified in 15 U.S.C. § 45(n).

9 First Amended Compl. for Injunctive and Other Equitable Relief at 19 ¶ 42, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR (D. Ariz. filed Aug. 9, 2012) (the complaint also alleged Wyndham engaged in "deceptive" acts, which is not discussed here).

10 Opinion of the Commission at *1, *In Re LabMD*, Docket No. 9357 (July 29, 2016).

11 *Id.*

12 Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 696 (7th Cir. 2015).

13 *Id.*

14 App. Reply Br. 34, Dec. 8, 2014, ECF No. 14-3514.

15 Pl.'s Br. 57, Nov. 5, 2014, ECF No.14-3514.

16 Initial Decision, In the Matter of LabMD Inc., 2015 FTC Lexis 135 at *200, No. 9357 (Nov. 13, 2015) (this decision was later reversed by an Opinion of the Commission).

17 *See, e.g.,* Liviu Arsene, *FTC Granted Authority as Corporate Cybersecurity Watchdog by US Court*, Hot for Security (Aug. 25, 2015), http://www.hotforsecurity.com/blog/ftc-granted-authority-as-corporate-cybersecurity-watchdog-by-us-court-12552.html [https://perma.cc/W7NG-M9V4].

18 15 U.S.C. § 45(a)(1) (Lexis 2015).

19 15 U.S.C. § 45(a)(2).

20 Wheeler-Lea Act of 1938, 75 P.L. 447, 52 Stat. 111, 75 Cong. Ch. 49 (Lexis 2015).

21 J. Howard Beales, Bureau of Consumer Protection, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection#N_7_ (last visited November 25, 2015, 8:48 PM) [https://perma.cc/MQH4-H5RS].

22 Statement of Basis and Purpose, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (1964).

23 The test is also referred to as the "S&H Rule" or "Sperry's Rule". For purposes of this Note, I will refer to it as the "Cigarette Rule."

24 Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, *supra* note 22.

25 FTC v. Sperry & Hutchinson, 405 U.S. 233, n.5 (1972).

26 Beales, *supra* note 21 ("apparent approval"); John Harrington, Note, *Up in Smoke: The FTC's Refusal to Apply the "Unfairness Doctrine" to Camel Cigarette Advertising*, 47 Fed. Comm. L. J. 593 (1995) ("tacitly approved the criteria"); David Belt, *Should the FTC's Current Criteria for Determining "Unfair Acts or Practices" Be Applied to State "Little FTC Acts"?*, 2010 A.B.A. Sec. The Antitrust Source ("it is unclear whether the Court actually approved the criteria").

27 Beales, *supra* note 21.

28 *Id.*

29 *Id.*

30 *Id.*

31 Statement of Basis and Purpose, Labeling and Advertising of Home Insulation, 44 Fed. Reg. 50, 218 (1979).

32 *See* Letter from the FTC Commissioners to Sen. Ford and Sen. Danforth (Dec. 17, 1980) [hereinafter "Unfairness Policy Statement"], reprinted as an appendix to *International Harvester Co.,* 104 F.T.C. 949.

33 *Id.*

34 *Id.*

35 Beales, *supra* note 21.

36 15 U.S.C. § 45(n) (Lexis 2015).

37 Beales, *supra* note 21.

38 Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014).

39 A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, FTC, July 2008, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited Nov. 25, 2015, 8:50 PM) [https://perma.cc/8TBK-BV8B].

40 *Id.*

41 Solove & Hartzog, *supra* note 37.

42 *Id.*

43 *Id.*

44 *Id.*

45 *Id*.
46 Prepared Statement of the Federal Trade Commission, FTC, *Protecting Consumer Information: Can Breaches Be Prevented?* (Feb. 5, 2014), https://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf (last visited Nov. 25, 2015, 8:54 PM) [https://perma.cc/9XW2-CKVV].
47 FTC v. Accusearch, Inc., 570 F.3d 1187 (Lexis 2009); *Wyndham*, 799 F.3d 236; *LabMD*, 2015 FTC Lexis 272.
48 *LabMD*, 2015 FTC Lexis 272 at *200.
49 Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress, FTC, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (last visited Jan. 26, 2016, 10:36 PM) [https://perma.cc/BH3L-TEG3].
50 Elie Freedman, Article, *An Era of Rapid Change: The Abdication of Cash & the FTC's Unfairness Authority,* 14 PGH. J. Tech. L. & Pol'y 351 (2014).
51 *Id*.
52 Privacy Online, *supra* note 48.
53 *Id*.
54 Freedman, *supra* note 49.
55 *Id*.
56 Complaint, BJ's Wholesale Club, Inc. No. C-4148 (F.T.C. Sept. 20, 2005).
57 *Id*.
58 *Id*.
59 *Id*.
60 *Id*.
61 *Id*.
62 Michael Scott, Article, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 Admin. L. Rev. 127 (2008).
63 *BJ's Wholesale Club*, No. C-4148.
64 Press Release, FTC, *DSW Inc. Settles FTC Charges*, (Dec. 1, 2005), https://www.ftc.gov/news-events/press-releases/2005/12/dsw-inc-settles-ftc-charges (last visited Nov. 25, 2015, 8:55 PM) [https://perma.cc/W6ZD-A5KF].
65 Complaint, DSW Inc., No. C-4157 (F.T.C. Mar. 7, 2006).
66 *Id*.
67 *Id*.
68 *Id*.
69 *Id*.
70 *Id*.
71 *Id*.
72 *Id*.
73 Complaint, Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010).
74 *Id*.
75 *Id*.
76 *Id*.
77 *Id*.
78 Unfairness Policy Statement, *supra* note 31.
79 *Id*.
80 15 U.S.C. § 45(n).
81 Unfairness Policy Statement, *supra* note 31.
82 Consumer Financial Protection Bureau, *CFPB Supervision and Examination Manual*, Version 2.0, October 2012), http://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf (last visited Nov. 25, 2015, 8:56 PM) [http://perma.cc/XSX7-5HVE] (internal citations omitted).
83 *Wyndham,* 799 F.3d 236.
84 First Amended Compl. for Injunctive and Other Equitable Relief at *19, *Wyndham*, No. CV 12-1365-PHX-PGR (the complaint also alleged Wyndham engaged in "deceptive" acts, not discussed here).
85 *Id*.
86 *Id*.
87 *Id*.
88 *Id*.
89 FTC v. Wyndham Worldwide Corp,, 10 F. Supp. 3d 602, 609 (D.N.J. 2014).
90 First Amended Compl. for Injunctive and Other Equitable Relief at *19, *Wyndham*, No. CV 12-1365-PHX-PGR.
91 *Wyndham*, 799 F.3d at 242.
92 *Wyndham,* 10 F. Supp. 3d at 625.
93 *Id*. at 622.
94 *Id*. at 625.
95 *Id*.
96 *Id*. at 602 n.15.
97 *Id*. at 631.
98 *Id*. at 626.
99 *Wyndham*, 799 F.3d 236.
100 Appellant's Opening Br., 45, October 6, 2014, No. 14-3514.
101 *Id*.
102 *See infra* Part III.B.1.
103 Appellant's Opening Br., No. 14-3514 (*Remijas v. Neiman Marcus* was later reversed by 7th Circuit).
104 Brief for the FTC, 58-59, Nov. 5, 2014, No. 14-3514.
105 *Id*. at 59.
106 *Id*.
107 *Id*. at 60-61.
108 *Wyndham*, 799 F.3d 236 (The Third Circuit did not specifically address whether Wyndham's conduct violated 15 U.S.C. § 45).
109 Stipulated Order for Injunction at *4, *Wyndham*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 2:13-CV-01887-ES-JAD) (providing Wyndham's obligations in the settlement are in effect for 20 years).
110 *LabMD*, 2015 FTC Lexis 272.
111 *Id*. at *12.
112 *Id*. at *13.
113 *Id*. at *26.
114 *Id*. at *1.
115 Def.'s Mot. Dismiss, No. 9357 (Apr. 24, 2015).
116 LabMD, Inc. v. Tiversa, Inc., 509 Fed. Appx. 842 (11th Cir. 2013); LabMD, Inc. v. FTC, 776 F.3d 1275 (11th Cir. 2015); Tiversa Holding Corp. v. LabMD, Inc., 2014 U.S. Dist. LEXIS 166052 (W.D. Pa. Dec. 1, 2014).
117 Dan Epstein, *Hounded Out of Business by Regulators*, Wall St. J., Nov. 19, 2015, http://www.wsj.com/articles/hounded-out-of-business-by-regulators-1447978301 (last visited Nov. 25, 2015, 8:58 PM) [http://perma.cc/4RRY-2BVZ].
118 *LabMD*, 2015 FTC Lexis 272 at *50.
119 *Id*. at *51.
120 *Id*.
121 *Id*. at *67.
122 *Id*. at *66.
123 *Id*. at *14. The second incident involved documents that were found in the possession of alleged identity thieves; however, the court stated the FTC had failed to establish a causal connection between these documents and LabMD's network. There was also no evidence that this exposure had caused or would be likely to cause consumer harm.
124 *Id*. at *91.
125 *Id*. The FTC requested to re-depose Tiversa's CEO and allow its expert witnesses to revise their opinions based on the revised testimony, but these requests were denied.
126 *Id*. at *16.
127 *Id*. at *25-26. Judge Chappell rejected LabMD's argument that the burden of proof standard is "clear and convincing evidence"; instead, Judge Chappell stated the FTC "has the burden of proving each factual issue…by a preponderance of credible evidence." (p. 46).
128 *Id*. at *26.

129 *Id*. at *50.
130 *Id*. at *102-105.
131 *Id*. at *110.
132 *Id*. at *113.
133 *Id*. at *114.
134 *Id*. at *27.
135 *Id*. at *114-117.
136 *Id*. at *118.
137 Opinion of the Commission at *1.
138 *Id*. at 16.
139 *Id*.
140 *Id*. at 17.
141 *Id*. at 18-19.
142 *Id*. at 20-21.
143 *Id*. at 20.
144 *Id*. at 21.
145 *Id*. at 24-25.
146 *Id*. at 21-23.
147 Caroline C. Cease, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 Ala. L. Rev. 395, 397 (2014).
148 *Id*.
149 *Id*.
150 U.S. CONST. art. III, § 2.
151 Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).
152 Barry Goheen, *Expert Q&A: Standing in Data Breach Class Actions,* Practical Law (Mar. 27, 2015) (standing challenges are specifically made under FRCP 12(b)(1) or FCRP(h)(3)).
153 Miles Galbraith, *America the Virtual: Security, Privacy, and Interoperability in an Interconnected World*, 62 Am. U.L. Rev. 1365, 1376 (2013).
154 Cease, *supra* note 136.
155 *Id*.
156 *Id*.
157 *Id*.
158 *See e.g.,* Galbraith, *supra* note 142 (noting plaintiffs' harm and expenses incurred in data breach cases are analogous to those made by plaintiffs in cases involving toxic exposure, environmental harm, and defective medical devices).
159 Cease, *supra* note 136.
160 Galbraith, *supra* note 142.
161 *Id*.
162 *Id*.
163 Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).
164 *Id*. (affirming the district court's dismissal of the action, however, because damages could not be recovered as a matter of Indiana law).
165 Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).
166 *Id*.
167 *Id*.
168 Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3rd Cir. 2011) (noting that the risk of injury here is "even more attenuated" than the issue in *Lujan* because "it is dependent on entirely speculative, future actions of an unknown third party" rather than the actions of the plaintiffs).
169 *Id*. at 40.
170 *Id*.
171 *Id*.
172 *Id*. at 43.
173 *Id*. Also distinguishing future harm in data breaches from cases involving medical devices, toxic torts, and environmental issues because of the lack of bodily harm and ability to monetarily return plaintiffs to their original position.
174 Barry Goheen, *Expert Q&A: Standing in Data Breach Class Actions,* Practical Law (Mar. 27, 2015).
175 Clapper v. Amnesty International, 185 L. Ed. 2d 264, 268 (2013) (Respondents are interested parties including attorneys, human rights entities, and media organizations who allege to engage in communications with individuals that may be targeted and put under surveillance).
176 *Id*. at 268-269.
177 *Id*. at 269.
178 *Id.* at 270.
179 *Id*. at 264 (reversing the Second Circuit's holding that the respondents had demonstrated an "objectively reasonable likelihood" that their international communications would be intercepted in the future).
180 *Id*. at 271.
181 *Id*. at 290.
182 *Id*. at 291.
183 *Id*. at 295.
184 Goheen, *supra* note 163 (noting that Clapper has been used mostly to dismiss cases).
185 *Id*. (noting that most district courts in the Seventh Circuit have applied *Clapper*, not *Pisciotta*, whereas district courts in the Ninth Circuits have suggested *Clapper* does not overrule *Krottner*).
186 *Id*. *See e.g.,* Lewert v. P.F. Chang's China Bistro, No. 14-4787, 2014 U.S. Dist. LEXIS 171142 (N.D. Ill. Dec. 10, 2014) (finding speculation of future harm and mitigation expenses do not constitute "actual injury" or "imminent harm"); Green v. ebay Inc., No. 14-1688, 2015 U.S. Dist. LEXIS 58047 (E.D. La. May 4, 2015) (finding plaintiff has failed to allege facts he has suffered an "actual or imminent injury"); Peters v. St. Joseph Servs. Corp., 74 Supp. 3d 847 (S.D. Tex. 2015) (finding future injuries are speculative and hypothetical but not imminent, and as such, the plaintiff lacks standing because she has not alleged a cognizable injury under Article III jurisprudence); Storm v. Paytime, 90 F. Supp. 3d 359 (finding access of data by an unknown third party doesn't equate to "misuse" and the length of time that has passed without such misuse "undercuts the imminency requirement"); Galaria v. Nationwide Mutual Ins. Co., 998 F. Supp. (mere exposure of plaintiff's personal information did not result in any "adverse consequences apart from the speculative injury of increased risk of identity theft").
187 Moyer v. Michaels Stores, Inc., No. 14-C561, 2014 U.S. Dist. LEXIS 96588, at *3 (N.D. Ill. Jul. 14, 2014).
188 *Id*. at *12
189 *Id*. at *15 (disagreeing with the defendants and other courts that *Clapper* overrules *Pisciotta*'s holding and imposes a stricter "imminent" requirement).
190 *Id*. at *19 (ultimately dismissing plaintiffs' claims despite a finding of standing because they had failed to plead actual damages as required by Illinois law). *But see* Strautins v. Trustwsave Holdings, Inc., 27 F. Supp. 3d 781 (finding *Clapper* essentially overrules the Seventh Circuit's standard in Pisciotta).
191 *Id*. The court also gave credence to a separate complaint involving a NY resident who used her credit card at a Michaels store during the alleged time frame of the breach and approximately two weeks later, incurred fraudulent charges. Although she was not a party to the present litigation, the court found her allegations to "inform [the] analysis."
192 In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014) (involving a class action suit arising out of a "criminal intrusion into a computer network system" in which millions of customers' personal information was stolen. Of the eleven named plaintiffs, only one alleged unauthorized charges).
193 *Id*.
194 *Id*. at 962.
195 In re Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014).
196 *Id*. at 1213-1214.
197 *Id*. at 1206.
198 *Id*. at 1214-1215 (distinguishing from *Clapper*, in which there was not any evidence that international communications had been or needed to be monitored).
199 *Id*. at 1215.
200 *Id*.
201 *Id*.

202 *Id*. at 1216.
203 *Id*.
204 *Id*. In addition to finding standing, the court found mitigation costs as an "additional cognizable injury" in light of the fact that the future harm being mitigated was itself imminent.
205 *Remijas*, 794 F.3d 688.
206 *Id*. at 690.
207 *Id*.
208 Remijas v. Neiman Marcus, No. 14-C1735, 2014 U.S. Dist. LEXIS 129574, at *2 (N.D. Ill. Sept. 16, 2014) (plaintiffs also sued Neiman Marcus for failing to disclose notice of the breach immediately).
209 *Remijas*, 794 F.3d at 692 (plaintiffs also alleged financial loss for purchasing products at Neiman Marcus that they wouldn't have bought had they been aware of the store's lax cybersecurity practices, and loss of control over the value of their personal information; neither of these allegations are discussed here).
210 *Id*.
211 *Remijas*, 2014 U.S. Dist. LEXIS 129574, at *9.
212 *Id*.
213 *Id*. at *8 (permitting a "plausible" inference that others among the 350,000 customers may face an "impending risk" of fraudulent charges, but rejecting the notion that any of the 350,000 customers face a "certain impending" risk of identity theft).
214 *Id*. at *14.
215 *Remijas*, 794 F.3d at 692.
216 John Hutchins, *Keeping the Data-Breach Headlines in Perspective*, JD Supra Business Advisor, (Oct. 22, 2015), http://www.jdsupra.com/legalnews/keeping-the-data-breach-headlines-in-29514/ [https://perma.cc/CP6X-N8KN].
217 *Remijas*, 794 F.3d at 693.
218 *Id*. at 694 (specifying "Clapper was addressing speculative harm based on something that may not even have happened to some or all the plaintiffs. In our case, Neiman Marcus does not contest the fact that the initial breach took place").
219 *Id*. at 693.
220 *Id*.
221 *Id*.
222 *Id*. at 694.
223 Spokeo v. Robins, 136 S. Ct. 1540, 1545 (2016).
224 *Id*.
225 *Id*. at 1544. Spokeo is a Web site that provides users with personal information about other individuals. Robins asserts Spokeo incorrectly published information pertaining to his marital status, age, occupation, and education.
226 *Id*. at 1554.
227 *Id*.
228 *Id*. at 1542.
229 Robins v. Spokeo, Inc., 742 F.3d 409, 412 (9th Cir. 2014).
230 *Spokeo*, 136 S. Ct. at 1550.
231 *Id*. at 1548.
232 *Id*. at 1549.
233 Such as phone number versus social security numbers.
234 For example, a laptop versus an online database.
235 Such as providing credit monitoring services or identity theft insurance.
236 Respondent LabMD, Inc.'s Application for Stay of Final Order Pending Review by a United States Court of Appeals, *In Re LabMD*, Docket No. 9357 (Aug. 30, 2016).