2018-2019

SOUTHERN ILLINOIS UNIVERSITY

NATIONAL HEALTH LAW MOOT COURT COMPETITION

Transcript of Record

Docket No. 18-251

BARKER & TODD, INC.,

Petitioner,

v.

Anthony Hope,

Respondent.

COMPETITION PROBLEM

SPONSORED BY:

Southern Illinois University School of Law

and

Department of Medical Humanities
Southern Illinois University School of Medicine

The American College of Legal Medicine

The American College of Legal Medicine Foundation

THIS PAGE INTENTIONALLY LEFT BLANK

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MISSOURIANA

Anthony HOPE, Plaintiff	)	
	)	No. AM-16-410-CV
v.	)	
	)	
BARKER & TODD, INC., Defendant.	)	

MEMORANDUM OPINION

TURPIN, District Judge

This matter comes before the Court on Defendant's motion to dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Defendant Barker & Todd, Inc. (B&T) is a pharmaceutical company that is incorporated and has its principal place of business in the state of Missouriana. Plaintiff Anthony Hope, a citizen of South Illinois, filed this class-action complaint against defendant on February 15, 2016, invoking diversity jurisdiction under 28 U.S.C. § 1332(d)(2). Plaintiff's complaint asserts common law negligence claims against the defendant, individually and on behalf of the putative class of similarly situated persons, for failing to safeguard their electronic protected health information (ePHI), based on standards set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Plaintiff asserts damages in excess of $5,000,000.[1]

I. FACTUAL AND PROCEDURAL HISTORY.

The following facts, as well-pleaded in the complaint, are treated as undisputed for purposes of this motion. This case arises out of a "security incident" experienced by B&T, a

[1] B&T does not at this time challenge the amount in controversy, the diversity of citizenship, the makeup of the putative class, or whether Plaintiff can meet the procedural requirements to assert a class action suit.

pharmaceutical company, that may have resulted in unknown individuals gaining unauthorized access to certain electronically stored personal health information. B&T manufactures several prescription drugs, a number of which are only partially covered by medical insurance. To offset the cost of taking its drugs, B&T offers a prescription assistance program for eligible participants.[2] The exact benefits of the program vary depending on the drug, but most offer either three or six-month supply of the drug for no cost. The participant must complete an application form, which asks for personal information including income, date of birth, social security number, medical insurance policy numbers, and medical history regarding the prescribed medication.

B&T stores this information electronically in encrypted form. This encryption allowed only devices with a proper decryption key to access data on the server. B&T further restricted access to the data by requiring users to sign into the authorized devices with a password. On October 26, 2015, B&T began an upgrade of its technology that involved moving its data from local servers to new private cloud-based servers, which it had purchased from an outside vendor. A B&T IT employee working on the data transfer failed to check for server updates prior to starting the transfer. This was a problem because servers are vulnerable to so-called "zero-day" exploits, which are holes in a server's security that are discovered and exploited by attackers before developers become aware of the problem and can issue a patch. Once the security vulnerability becomes known, attackers write exploits that target servers that have not been updated since the patch was released (called "n-day" exploits, "n" being the number of days between when the exploit is discovered and the security patch is installed). The vendor in this case had discovered

[2] Eligibility depends on such things as the participant's monthly income and the participant not having any other form of coverage for the drug through a government program or third party insurer.

an exploit that allowed unauthorized users to access its cloud servers without needing the decryption key, and it issued a patch shortly after B&T purchased the servers.

Once the IT department discovered the servers had not been updated, they installed the patch, which eliminated any on-going threat from the exploit. Some data from one particular local server had already been transferred to an un-patched cloud server, however, and that data was vulnerable to the exploit for approximately 8 hours. That data included the files for participants in the prescription drug access program for B&T's newest arthritis drug, Flexacor. As required under HIPAA's regulations, 45 C.F.R. § 164.404(b) (2015), and Missouriana's Data Breach Notification Act, 410 M.C.S. § 22/45–101(a) (2010), B&T sent out a notification on November 8, 2015, about a potential electronic protected health information (ePHI) breach to the involved participants.[3] *See generally* 45 C.F.R. § 160.103 (2015) (defining electronic protected health information as individually identifiable health information transmitted by electronic media). B&T explained in its notice that it was not clear whether any ePHI had actually been accessed, but B&T was continuing to investigate. In order to address the possible risk of identity theft, B&T offered the affected participants a year of free credit monitoring.

Plaintiff Anthony Hope was one of the participants who received notice that his ePHI may have been accessed. He then immediately signed up for the credit monitoring B&T offered. The credit monitoring company alerted Mr. Hope on November 30, 2015, that it found the account user name and password he had used for his B&T account, his date of birth, and his social security number on the dark web,[4] on a "darknet market" website with a download counter indicating files with his information had been downloaded hundreds of times. To date, Mr. Hope

[3] B&T determined that the total number of potentially affected participants was 426.

[4] The dark web is that part of the internet that is not indexed by search engines and requires a special browser to access. Darren Guccione, *What is the dark web? How to access it and what you'll find*, CSO from IG (Jan. 19, 2018), https://www.csoonline.com/article/3249765/data-breach/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.

has not experienced any fraudulent credit charges or any other incidents suggesting someone has appropriated his identity.[5] Hope alleges he has experienced a considerable amount of fear and anxiety about the prospect of his identity being stolen, especially since he is getting married soon and he and his new husband will be combining their finances.

Hope filed this class action suit against B&T on February 15, 2016, on behalf of himself and other consumers whose ePHI was similarly found on the dark web. Hope asserts that under Missouriana law, he and other members of the class are entitled to damages from B&T for its negligent handling of their ePHI. Hope specifically alleged that B&T was negligent per se because its actions violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.), and its implementing regulations, 45 C.F.R. §§ 164.302-.318 (2015), because B&T failed to properly secure his ePHI. Hope also alleged B&T's actions amounted to general negligence, again based on its violation of HIPAA.

B&T filed its answer to the complaint on March 1, 2016, along with Motions to Dismiss under Federal Rule of Civil Procedure 12(b)(1) for lack of standing and 12(b)(6) for failure to state a claim upon which relief may be granted. In its 12(b)(1) motion, B&T alleges that the plaintiff class has failed to establish injury-in-fact for purposes of Article III standing. In its 12(b)(6) motion, B&T alleges that HIPAA violations may not properly form the basis for either a negligence per se or general negligence claim under Missouriana law. B&T requests the Court dismiss the complaint. This Court finds that the plaintiff class does not have standing as the matter is currently plead, and that even if the plaintiff could establish standing, he has failed to

[5] Hope put a credit freeze in place, which requires him to be notified if someone attempts to open a new account using his credentials. Hope must go through several steps to remove that freeze if he wishes to obtain new credit of any kind.

state a claim upon which relief may be granted to the putative class. Accordingly, the Court grants B&T's motions to dismiss.

II. DEFENDANT'S MOTION TO DISMISS FOR LACK OF STANDING

B&T argues that the plaintiff class does not have standing to file this lawsuit because the plaintiff class does not have an injury-in-fact sufficient for standing under Article III of the United States Constitution. B&T, therefore, argues this suit should be dismissed under Federal Rule of Civil Procedure 12(b)(1) for lack of subject matter jurisdiction.

Motions to dismiss for lack of standing are reviewed under the requirements of Federal Rule of Civil Procedure 12(b)(1), as lack of standing means a court lacks subject matter jurisdiction. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). Plaintiffs have the burden of showing subject matter jurisdiction and must prove that it exists by a preponderance of the evidence. *Id.* at 561.

The Supreme Court has stated that "Article III of the Constitution limits federal courts' jurisdiction to certain 'Cases' and 'Controversies.'" *Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 408 (2013). One piece of the "case and controversy" requirement is the plaintiff's standing to sue. *Id.* The party who invokes federal jurisdiction, in this case the plaintiff, has the burden of showing that standing exists. *Id.* at 412; *see also Hollingsworth v. Perry*, 570 U.S. 693, 704 (2013) (requiring that "any person invoking the power of a federal court must demonstrate standing to do so"). There are three requirements to standing: the injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010). Only the first requirement is at issue in this case. As noted, the first requirement, generally called "injury-in-fact," has two elements – it must be "concrete and particularized" and "actual or

imminent." *Id.* The injury cannot be "conjectural or hypothetical." *Lujan*, 504 U.S. at 560. B&T alleges Hope has failed to establish the putative class suffered injury-in-fact, and the Court agrees.

Hope contends the putative class's injury is concrete and particularized enough to establish injury-in-fact because their ePHI has been made available for sale on the dark web, and as a result, they suffer from an increased risk of identity theft and an increased risk of fraud as a direct result of defendant's negligent actions. Hope argues this risk of future harm, and the actions they must take to guard against it, are substantial and impending enough that the harm is neither conjectural nor hypothetical. The issue of whether an increased risk of identity theft or fraud due to a data breach resulting in theft of personal information is a particularized injury that establishes injury-in-fact is a matter of first impression in this circuit. We first turn to the Supreme Court's most recent relevant interpretation of injury-in-fact.

In *Clapper,* the Supreme Court considered whether future injury will satisfy the injury in fact requirement. *See Clapper,* 568 U.S. at 410. The Court ruled that "[t]hreatened injury must be certainly impending to constitute injury in fact." *Id*. The court rejected "allegations of possible future injury" as insufficient. *See id.* While the Supreme Court did note that injury need not always be "literally certain," it reasoned that standing is not conferred if the theory of injury-in-fact "relie[s] on a highly attenuated chain of possibilities." *Id.*

Defendant B&T cites *Clapper* and other lower court opinions that ruled increased risk of identity theft is not in itself sufficient for injury-in-fact in a data breach case. For example, the First Circuit ruled that increased risk of harm in a data privacy case was too conjectural to constitute injury-in-fact for Article III purposes. *Katz v. Pershing, LLC,* 672 F.3d 64, 79-80 (1st Cir. 2012). The Third Circuit also ruled that increased risk of identity theft alone does not meet

the requirement for Article III standing. *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011).

Hope argues that the putative class members' injury is concrete and particularized enough to establish injury-in-fact because their information was found on the darknet market, which shows it has been compromised by individuals who intend to use it nefariously. Hope argues this has led him and other members of the class to suffer from the increased need to monitor their credit and other personal affairs potentially vulnerable to identity theft, as well as from the anxiety and stress related to possible identity theft. Hope also asserts that although B&T paid for one year of credit monitoring, it is not clear that one year will be sufficient, especially in light of the fact his data has been downloaded hundreds of times so far. He and the other class members may, therefore, incur additional expenses related to credit monitoring after B&T's offer expires.[6] This Court finds that fear and anxiety surrounding the risk of future fraud or identity theft are injuries that are too speculative to meet the requirements for injury-in-fact as set forth in *Clapper*. Injury based on future speculative injury is simply not sufficient. Further, because the alleged injury of the risk of future fraud or identity theft are too speculative, costs associated with that speculative risk also do not show injury-in-fact.

In this case, the alleged injury-in-fact is based on a chain of possibilities. While their information was found on the dark web, the putative class does not allege any actual misuse of the data. Similar to the cases referenced above, in order for actual misuse to occur, many actions must first take place for any member of the putative class to suffer injury-in-fact. For example, the data attacker must continue to place Hope's ePHI on the dark web, and there must be a person on the dark web who will not only purchase Hope's ePHI but use it successfully, even though Hope has a credit monitoring service. This Court finds Hope and the other class

[6] B&T has not indicated if it is willing to extend its offer for those whose data has been found on the dark web.

members are similarly situated to the plaintiffs in the cases discussed above in that they have not yet experienced injury-in-fact.

Therefore, for the reasons discussed, this Court concludes Hope has not sufficiently established injury-in-fact to meet the requirements of Article III standing. The Court recognizes that in cases involving constitutional standing, the Court may permit the plaintiff an opportunity to amend his complaint to provide additional support for his assertion of standing. *See Warth v. Seldin*, 422 U.S. 490, 501 (1975) ("[I]t is within the trial court's power to allow or to require the plaintiff to supply, by amendment to the complaint or by affidavits, further particularized allegations of fact deemed supportive of plaintiff's standing."). In this case, however, because the Court also finds Hope failed to state a claim upon which relief can be granted, as addressed below, the Court instead dismisses the complaint without prejudice.

III. DEFENDANT'S MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM

To survive a motion to dismiss, a plaintiff must allege facts with sufficient specificity to state a claim for relief that is plausible on its face. *Ashcroft v. Iqbal*, 556 U.S. 662, 678–79 (2009). The Court must accept as true all factual allegations, but the Court does not apply this presumption of truth to conclusory or legal assertions. *Id.* at 678–79. Hope asserts two legal theories for holding B&T liable for injuries arising from the data breach. First, Hope alleges B&T's actions violated duties it owed under HIPAA's statute and regulations, which amounts to negligence per se. Second, Hope alleges B&T's actions were unreasonable under negligence law in general because HIPAA establishes a standard of care as to what is reasonable. The Court does not believe Missouriana would recognize either theory, and finds as a matter of law Hope has failed to state a claim upon which relief may be granted.

Hope points to several HIPAA regulations he alleges articulate a standard of care for the defendant's actions in this case. First, Hope cites HIPAA's general privacy rule, which requires covered entities ensure all electronic protected health information they create, maintain, or receive is kept confidential. *See* 45 C.F.R. § 164.306(a)(1) (2015). Second, Hope cites the security standards located in the HIPAA regulations. *See* 45 C.F.R. § 164.312 (2015). Hope contends that B&T is a covered entity that failed to maintain ePHI so that only authorized individuals were able to access that information. *See id.* § 164.312(a)(1) (requiring covered entities implement technical policies and procedures to control access to ePHI); *see also id.* § 160.103 (defining covered entity). This includes "[i]mplement[ing] a mechanism to encrypt and decrypt electronic protected health information." *Id.* § 164.312(a)(2)(iv). Hope alleges that had B&T followed proper policies and procedures to maintain the electronic records in encrypted format, the security breach would not have occurred.

Hope indicates while he is alleging B&T violated HIPAA, he is not bringing a claim under HIPAA itself, as he concedes that HIPAA does not support a private cause of action. *See Adams v. Eureka Fire Prot. Dist.*, 352 Fed. Appx. 137, 138–39 (8th Cir. 2009) ("Courts have repeatedly held that HIPAA does not create a private right in implied-right-of-action cases."). Instead, Hope asserts courts may look to HIPAA's standards to determine the state law standard of care to protect personally identifiable patient information. *See I.S. v. Washington Univ.*, No. 4:11CV235SNLJ, 2011 WL 2433585, at *2 (E.D. Mo. June 14, 2011) (allowing plaintiff's claim to stand as referencing HIPAA to provide the standard of care to use in judging the defendant's actions). Hope thus first alleges that B&T's violation of HIPAA's regulations amounts to negligence per se. Missouriana has adopted a statute codifying negligence per se doctrine:

> An actor is negligent if, without excuse, the actor violates a statute that is designed to protect against the type of accident the actor's conduct causes, and if the accident

victim is within the class of persons the statute is designed to protect.

302 M.C.S. § 3/22-104 (2014). Missouriana has not yet ruled, however, on whether it would recognize violation of a federal statute or regulation as the basis for a negligence per se claim. We recognize that some states have allowed negligence per se claims based on HIPAA violations. *See, e.g., I.S.*, 2011 WL 2433585, at *2 (holding that plaintiff's claim "may stand as a state claim for negligence per se despite its exclusive reliance upon HIPAA"). We find, however, the reasoning of cases rejecting similar claims more persuasive.

For example, the Ohio Court of Appeals has recently concluded that HIPAA's lack of a private cause of action ruled out using that statute and its regulations to establish negligence per se. *Sheldon v. Kettering Health Network*, 40 N.E.3d 661, 672 (Ohio Ct. App. 2015). That court reasoned that "federal regulations—as opposed to [a state] statute that sets forth a positive and definite standard of care—cannot be used as the basis for negligence per se." *Id.* Moreover, allowing such a claim would be "tantamount to authorizing a prohibited private right of action for violation of HIPAA itself." *Id.* The history of HIPAA itself supports the Ohio court's interpretation, in that HIPAA originally permitted only the Department of Health and Human Services (HHS) to enforce the Act, and when the statute was amended by the HITECH Act in 2009,[7] Congress added only the additional authority for states Attorneys General to also enforce the Act. *See* 42 U.S.C. § 1320d-5(d) (2009).

There is a significant reason besides HIPAA's preferred enforcement mechanism that calls for the court to reject the claims. HIPAA distinguishes between standards that require certain steps and those which identify only "addressable" issues. *Compare* 45 C.F.R. § 164.312(a)(2)(i) (2012) (requiring entities assign a unique name or number to identify and track

[7] American Recovery and Reinvestment Act of 2009, Pub. L. 111-5 (Feb. 17, 2009).

user identity) *with id.* § 164.312(a)(2)(iii) (suggesting covered entities to implement procedures that terminate an electronic session after inactivity by using the word "addressable"). In the case of encryption of ePHI, HIPAA does not actually require the records to be encrypted, let alone encrypted at all times as plaintiff alleges. *See id*. § 164.312(a)(2)(iv). Rather, HIPAA regulations indicate that encryption is only an addressable standard, which means that covered entities should assess whether implementing encryption is a "reasonable and appropriate safeguard in its environment," and implement encryption "if reasonable and appropriate." *Id*. § 164.306(d)(3)(i). The flexibility here does not provide a standard upon which a negligence per se claim may be based. *See Sheldon*, 40 N.E.3d at 674 (rejecting a similar attempt to imply a duty to perform security audits).

Perhaps recognizing this, Hope also frames his claim as arising under general negligence law, which would ask whether B&T acted reasonably under the circumstances. This claim, however, does not fare any better. Hope has not identified a basis in Missouriana law for imposing a duty of care on pharmaceutical companies to keep ePHI private. Some courts have looked to HIPAA to inform the standard of care, but in those cases, there was underlying state law recognizing the defendant's duty. For example, the Connecticut Supreme Court reasoned that "to the extent that Connecticut's common law provides a remedy for a health care provider's breach of its duty of confidentiality[,] . . . regulations . . . implementing HIPAA may inform the applicable standard of care." *Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*, 314 Conn. 433, 436 (2014). Missouriana has not recognized, in its common law or statutory law, a duty by pharmaceutical companies to hold customer information confidential. Missouriana statutory law requires "health care providers" maintain patient record confidentiality but defines "health care provider" to include only "physicians; surgeons; podiatrists; dentists; optometrists;

psychologists; physical or occupational therapists; marriage, family and child counselors; clinical social workers, and any other health care professional licensed under Missouriana law." 58 M.C.S. § 10/5-101 (2008). Hope concedes this statute, on its face, does not impose a duty on pharmaceutical companies, and thus does not supply a basis for finding a duty of care owed to the putative class in this case. Hope fares no better by pointing instead to the Missouriana Data Breach Notification Act, which applies to "[an] individual or a commercial entity that conducts business in Missouriana and that owns or licenses computerized data that includes personally identifiable information about a resident of Missouriana." 410 M.C.S § 22/46-101(a) (2005).[8] While that statute clearly applies to B&T and the electronic records in this case, the statute requires only that the entity "conduct in good faith a reasonable and prompt investigation to determine the source of the breach," *id.* § 22/46-103(a), and "give notice as soon as possible to the affected Missouriana resident," *id.* § 22/46-103(b). Nothing in the statutory language creates any duty beyond that of notification.

What Hope is trying to do is bootstrap a HIPAA claim into a state law negligence claim to create a duty where none currently exists in Missouriana law. Hope's negligence theory in this case is that B&T had a duty to maintain its patient records at all times in an encrypted format that could not be accessed by any unauthorized individuals, a duty it breached when the records were left briefly unencrypted during the upgrade to the cloud based servers. But, HIPAA does not require that. It requires that the covered entity to guard against unauthorized access but does not require encryption, only whenever the entity deems it appropriate. *See* 45 C.F.R. § 164.312(e)(2)(ii) (2015) (referring to encryption as an "addressable" standard). Whether a covered entity violates this duty requires assessment by HHS, whereas here, Hope asks the Court

[8] The Missouriana Data Breach Notification Act also states "[t]he Missouriana Attorney General may investigate violations and levy civil penalties if it finds a covered entity has violated any provision of this [Act]." 410 MCS § 22/46-104(a) (2005).

to base liability on failure to comply with standards deemed only "addressable" within HIPAA's regulations. Congress did not authorize a private right of action to enforce that standard, but the plaintiff will have in effect created such a cause of action. The Court does not think this is a proper use of HIPAA, especially given the lack of clear state law imposing a duty on this type of defendant.

Finally, the Court makes clear what it is not ruling. Some cases have framed the issue as whether HIPAA preempts state law negligence claims for breach of confidentiality duties. *See Byrne*, 314 Conn. at 445 (analyzing whether HIPAA preempts state law negligence claims); *see also* 42 U.S.C. § 1320d–7 (a)(1) (2010) (preempting state laws that are "contrary" to HIPAA's standards). The Court finds that preemption is not the question here because Hope is asking the Court to follow HIPAA, not some independent state law that may supply a contrary set of substantive standards. In fact, that is Hope's problem—he does not point to an independent state law basis for finding the pharmaceutical company owed the plaintiff class a duty to maintain their records in encrypted form at all times.

Therefore, because the Court does not believe Missouriana would find negligence per se when the underlying statute does not create a private right of action or a clear obligation, the Court finds that Hope has failed to state a negligence per se claim as a matter of law. Hope also fails to state a common law negligence claim upon which relief can be granted, for much the same reasons. Hope did not assert an independent state law duty that B&T owed to individuals who voluntarily participated in the prescription assistance program. Because his claims rest solely on HIPAA to create the standard of care, Hope has failed to state a claim upon which relief may be granted.

ORDER

For the foregoing reasons, Defendant's Motions to Dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) are GRANTED. The Complaint is DISMISSED without prejudice.

IT IS SO ORDERED.

_____

Honorable Judge Turpin, District Judge
April 30, 2016

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRTEENTH CIRCUIT

No. 17-1450

Anthony Hope, *Appellant*

v.

BARKER & TODD, INC. *Appellee*

Appeal from the United States District Court for the District of Missouriana
No. AM-16-410-CV – Turpin, Judge

Argued June 13, 2017 – Decided December 22, 2017

Before: Bamford, Pirelli, Ragg, Circuit Judges,

BAMFORD, Circuit Judge:

Appellant Anthony Hope filed this class action suit against Appellee Barker & Todd, Inc. (B&T) under the federal court's diversity jurisdiction, alleging Missouriana state law negligence claims for a breach of electronic protected health information (ePHI) held by B&T. The complaint alleged that B&T breached its duties to the putative class under the Health Insurance Portability and Accountability Act (HIPAA)'s standards. *See* 45 C.F.R. §§ 164.306, 164.312 (2017) (outlining regulations covered entities must follow regarding general privacy requirements and technical safeguards); *see also* HITECH Act, 42 U.S.C. §§ 1320d-2(d), 1320d-5(d) (2012) (allowing the secretary of the Department of Health and Human Services to create regulations that conform to HIPAA standards, and giving state Attorney Generals the authority to pursue civil action on behalf of residents of their state if affected by an entity who has violated

the regulations). B&T moved to dismiss the complaint on two grounds: that 1) under Federal Rule of Civil Procedure 12(b)(1), the putative class lacked Article III standing to sue in regard to the data breach because there was no injury-in-fact; and 2) under Federal Rule of Civil Procedure 12(b)(6), Hope failed to state a claim upon which relief can be granted because he improperly asserted violation of HIPAA as the basis for state law negligence claims. The United States District Court for the District of Missouriana granted the motions and dismissed the complaint without prejudice. Hope appealed the district court's order dismissing the complaint.

We find that the district court dismissed Hope's complaint in error. Hope, on behalf of the putative class, has alleged sufficient injury-in-fact to establish Article III standing to sue, and the complaint does allege a claim upon which relief may be granted. Accordingly, we reverse and remand this matter to the district court.

BACKGROUND

The parties do not dispute the relevant facts in the record, but instead dispute the interpretation and application of the legal standards in this case. The district court gave a thorough account of the facts in its memorandum opinion, and we now incorporate its articulation of those facts for this opinion. Briefly, Hope and the other members of the putative class all participated in B&T's prescription assistance program for the arthritis drug Flexacor. In the process of upgrading its technology, B&T for a time left the class's ePHI vulnerable to breach by individuals not authorized to gain access to that information. Hope, similar to the other class members, has found his information on a dark web "darknet market" website that shows it has been downloaded hundreds of times. Hope does not allege there have been any fraudulent credit charges or actual incidents of the class members' identities being used for unauthorized purposes. Hope contends that because his ePHI was accessed by an authorized

user who placed it for sale on the dark web, he has standing to sue B&T for breach of a duty it owed to keep that information private and secure. He further contends that he may properly base his state law negligence claims on B&T's failure to comply with HIPAA's provisions requiring covered entities to maintain the privacy of ePHI and secure that data from unauthorized access through appropriate means, including encryption.

The district court found the putative class lacked standing because no member of the class had shown any concrete harm from the breach that occurred at the clinic, thus failing to meet Article III's requirement to show injury-in-fact. The district court alternatively considered B&T's 12(b)(6) motion to dismiss, and concluded the complaint failed to state a claim upon which relief could be granted because state law negligence claims may not be based on violation of HIPAA standards. The district court dismissed Hope's complaint without prejudice on April 30, 2016. Hope filed a timely notice of appeal in this Court on May 25, 2016. The parties submitted briefing and presented oral argument. We now turn to the resolution of these appeals.

DISCUSSION

I. ARTICLE III STANDING

We review a district court's grant of a motion to dismiss under Federal Rule of Civil Procedure 12(b)(1) *de novo,* because the issue of jurisdiction is one that each court has an independent obligation to consider. *Arbaugh v. Y&H Corp.*, 546 U.S. 500, 514 (2006). The district court properly stated the standards guiding its decision as equivalent to those applied in Federal Rule of Civil Procedure 12(b)(1) motions to dismiss. It also correctly outlined the three basic requirements for standing: (1) injury-in-fact, (2) causation, and (3) redressability. *See Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992). B&T contends that Hope has failed to

establish the putative class suffered a "concrete and particularized" injury as required for Article III standing. The district court agreed, but we do not.

The court below relied heavily on *Clapper v. Amnesty International USA,* 568 U.S. 398 (2013), and, because it is an issue of first impression in this Circuit, various other circuit court decisions holding possible identity theft resulting from a data breach is a future harm that is too speculative to meet the constitutional requirements for injury-in-fact. *See, e.g., Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (concluding allegations of "hypothetical, future injury" from data breach are not sufficient). Subsequent to the district court's decision, the United States Supreme Court revisited the issue of how concrete the alleged injury-in-fact must be, in *Spokeo, Inc., v. Robins,* 136 S.Ct. 1540, 1548-49 (2016). We find the Supreme Court's reasoning in *Spokeo* most relevant in this case, in favor of finding standing.

In *Spokeo,* the plaintiff sued under the Fair Credit Reporting Act of 1970, alleging under 15 U.S.C. § 1681e(b), defendant Spokeo failed to "'follow reasonable procedures to assure maximum possible accuracy of' consumer reports" maintained on its website. *Id.* at 1553-54. The plaintiff specifically alleged that information in a profile about him generated through Spokeo's "people search engine" contained inaccurate information about, among other things, his marital status, his age, and his education. *Id.* at 1546. In his amended complaint, he alleged non-tangible injuries including employment difficulties and stress and anxiety. *Id.* at 1556. The district court dismissed his complaint with prejudice, but the Ninth Circuit reversed because it found his injuries were sufficiently "particularized" in that they were individualized and alleged a violation of his own rights, not only the statutory rights of other individuals. *See id.* at 1546 (explaining lower courts' reasoning).

The Supreme Court remanded the case but did not decide whether the plaintiff had standing; instead, the Court held that the Ninth Circuit failed to analyze properly the injury-in-fact requirement. *Id.* at 1550. In doing so, however, the Court clarified the procedure to determine whether a non-tangible injury is sufficient for standing purposes. *See id.* at 1549 (explaining that intangible injuries are sometimes concrete enough for standing purposes). The Court reasoned that "particularized" and "concrete" are two separate requirements of injury-in-fact; they are not considered as one element that can be satisfied by meeting either requirement. *Id.* at 1549. The Court also reasoned that the concreteness requirement "does not mean . . . that the risk of real harm cannot satisfy that requirement." *Id.* at 1543. Intangible injuries can be concrete enough for standing, but the Court also made clear that "the demands of Article III . . . cannot be satisfied by a bare procedural violation." *See id.* at 1549 (reasoning that while a violation of a procedural right may be sufficient for injury in fact, a "bare procedural violation, divorced from any concrete harm" would not be sufficient). The Court found it instructive to look to "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* Under this reasoning, injuries that consist of a risk of future identity theft or fraud arising from an identifiable data breach and not bare procedural violations, and may satisfy the concreteness requirement to meet the injury-in-fact element of Article III standing.

Some circuit courts analyzing intangible injuries post-*Spokeo* have held the breach of personally identifiable information and the resulting risk of future identity theft or fraud, as well as the fear and anxiety included with this risk, are sufficiently "concrete" to meet the requirements of Article III standing. Implicitly rejecting its *Reilly* decision, the Third Circuit recently held that plaintiffs established injury in fact in their suit for violation of the Fair Credit

Reporting Act, in part because of the long-standing recognition that unauthorized disclosures of personal information is injurious and not a bare procedural violation of the statute. *See In re Horizon Healthcare Servs. Inc. Data Breach Litig,* 846 F.3d 625, 638-39 (3d Cir. 2017) (finding injury in fact after two laptops were stolen from the defendant's office, compromising the plaintiff's protected and personally identifiable information). The Third Circuit concluded the harm resulting from unauthorized disclosure of personal information was closely related to the harm of invasion of privacy, which is traditionally allowed as a basis for a lawsuit, and thus the harm was concrete. *See id.* at 639; *but see Beck v. McDonald,* 848 F.3d 262, 275 (4th Cir. 2017) (continuing to require future identity theft be "sufficiently imminent" in case where plaintiffs had no evidence stolen laptops had been accessed).

Here, the injury Hope alleges meets the *Spokeo* standard. The disclosure of ePHI, which could lead to identity theft or fraud, is a harm that Congress intended to protect with various statutes, including HIPAA. While we acknowledge that HIPAA itself does not create a private right to sue, as we discuss below under Issue II, the unauthorized disclosure of personally identifiable health information is closely linked with an invasion of one's privacy, which has traditionally been a harm entitling a plaintiff to relief in English or American common law. In other words, there is a case and controversy given the type of invasion that has occurred here.

Moreover, Hope's situation differs from cases where the plaintiffs failed to show their personal information was targeted. Here, Hope and the other plaintiffs' ePHI has been found on the dark web, being downloaded hundreds of times. That information includes their dates of birth and their social security numbers, in addition to medical provider information—the stuff of dreams for identity thieves. Accordingly, even under *Clapper's* analysis, the plaintiffs have a sufficient concrete and particularized injury, not a mere conjectural one. The district court,

relying on the fact that Mr. Hope had no tangible injury, ignored significant differences in the cited cases. For example, in *Reilly v. Ceridian Corp.,* the Third Circuit found no standing, but its reasoning was based on it being unclear whether the attacker had read, copied, or understood the information. *Reilly,* 664 F.3d at 38. Here, Hope has alleged an identifiable taking and use of his personal data. Moreover, it is not appropriate to make Hope wait for a fraudulent credit card charge or identity theft because his information has already been found for sale on the dark web. Hope's risk of identity theft is higher than it would be for someone whose data may have been vulnerable due to a security incident but there is no evidence whether that data was read or whether the attacker intended to make use of it. Because Hope alleged a theft of personally identifiable information that was later found for sale on the dark web, we hold that he does have an injury-in-fact sufficient for Article III standing to sue.

Therefore, we find Appellant Hope has sufficiently pled an injury-in-fact as required for Article III standing. The facts alleged show that B&T failed to protect the putative class's ePHI and that information was obtained by an unknown attacker and made available to other unauthorized users. The putative class has suffered an intangible harm that this Court recognizes as sufficiently concrete and particularized to establish injury-in-fact for standing. The district court, therefore, erred in finding the putative class lacked standing.[9]

II. State Law Negligence Claims Based on HIPAA Standards

The district court alternatively found that the complaint did not assert a claim upon which relief could be granted, because the court found it to improperly assert violation of HIPAA's standards as the basis for the standard of care owed the putative class to protect their ePHI. We

[9] B&T has raised no issues about either causation or redressability, and we see no basis to reject standing on either of those grounds. The putative class's information was found on the dark web within a month of the data breach, and the plaintiffs seek monetary damages to compensate for the harm caused by the unauthorized access to their ePHI.

find the district court took a far too cabined view of the nature of Hope's assertions. Hope alleges that HIPAA may inform the standard of care in a state negligence proceeding. We see nothing in Missouriana state law that would preclude such an approach. While no cases have directly addressed the issue, Missouriana's negligence per se statute is directly based on the Restatement (Third) of Torts, which recognizes federal statutes and regulations can give rise to a finding of negligence per se. *See generally* Restatement (Third) of Torts: Phys. & Emot. Harm § 14 cmt. A (Am. Law Inst. 2010) (stating that the negligence per se section "most frequently applies to statutes adopted by state legislatures, but equally applies to . . . federal statutes as well as regulations promulgated by federal agencies"). Other federal courts, when presented with a similar question, have held that negligence per se claims may be based on violation of HIPAA. *See, e.g., K.V. & S.V. v. Women's Healthcare Network, LLC*, No. 07-0228-CV-W-DW, 2007 WL 1655734, at *1 (W.D. Mo. June 6, 2007) (holding plaintiff's negligence per se claim relying on HIPAA stated a cause of action). Thus, without a clear indication that Missouriana would hold differently, we reject the district court's conclusion HIPAA cannot form the basis for a Missouriana state law negligence per se claim.

Regarding the general negligence claim, Hope does not argue that B&T should be liable merely because it has violated HIPAA. Rather, Hope argues that B&T failed to comply with a state law duty to protect ePHI from unauthorized disclosure, and in assessing what a reasonable entity would have done to safeguard those personally identifiable records, the trial court may look to relevant HIPAA statutory and regulatory provisions for guidance. *See Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*, 314 Conn. 433, 459 (2014)(allowing HIPAA to inform the standard of care applicable to negligence claims). The district court is correct that there is no issue of preemption here, so we see no conflict in allowing HIPAA's provisions to inform the

court in a state law proceeding alleging the defendant failed to protect individuals' private health care records. *See* 45 C.F.R. § 160.203(b) (2017) (exempting state laws from HIPAA's preemption provision when they would provide greater protection to "the privacy of individually identifiable health information").

The district court found no state law obligation of a pharmaceutical company to safeguard personally identifiable health records, but that ignored the fact Missouriana has recognized that individuals have a general right of privacy in their medical records. See *Hanson v. Jones Medical Ctr.*, 199 Mis. 2d 321, 333 (2002) (holding medical center liable for public disclosure of private facts when it disclosed results of wife's pregnancy test to her estranged husband without her consent). Here, admittedly, the defendant is not a medical center and the lower court correctly recognized drug companies are not covered entities under Missouriana medical confidentiality laws. But that should not preclude us from finding a plausible state law negligence claim. *See, e.g., Ins. Co. of N. Am. v. English*, 395 F.2d 854, 860 (5th Cir. 1968) (reasoning that when there are no state cases on point, the federal court has a duty to "arrive at the decision which reason dictates, with the faith that the state courts will arrive at the same decision"). Missouriana has not so far had an opportunity to determine the scope of a pharmaceutical company's duty to encrypt patient records, but drug companies are (or certainly should be) familiar with their obligations under HIPAA. *See Byrne*, 314 Conn. at 460 (reasoning that "[because] Connecticut health care providers . . . follow the procedures required under HIPAA . . . HIPAA and its implementing regulations may be utilized to inform the standard of care"). Rather than creating confusion or undermining enforcement of HIPAA, using HIPAA's well-established regulations would in fact increase efficiency and provide guidance regarding

what is required to protect and secure personal information in the technological age of storing and transferring data electronically.

Thus, we hold that Appellant Hope has stated a plausible state law negligence claim upon which relief can be granted by asserting Appellee B&T failed to maintain the confidentiality of his and other class members' ePHI, resulting in unauthorized access. In determining the scope of B&T's duty to protect those records, the court may properly look to standards established under HIPAA. There are substantial questions of fact regarding whether B&T complied with HIPAA and for that reason, we REVERSE and REMAND this matter to the court below.

PIRELLI, dissenting

I dissent from my colleague's finding that the putative class has standing to sue. Contrary to the majority's finding that *Spokeo* supports finding injury-in-fact in this case, it does not. My colleagues too readily dismiss something I believe to have been fundamental to the Supreme Court's conclusion in that case—the plaintiffs there sued under the Fair Credit Reporting Act, which provides for a private cause of action to enforce the rights granted under that statute. *See* 15 U.S.C. § 1681n(a) (2012); *see also Spokeo v. Robins*, 136 S.Ct. 1540, 1549 (2016) (characterizing Congress's judgment to allow a private right of action as "instructive and important"). Congress has not granted a similar right under HIPAA, and without that right, I do not believe it sufficient to allege a mere intrusion, even if the records in question were private. Rather, the injury becomes concrete and particularized when those records are misused to the plaintiffs' detriment. The district court correctly dismissed this case without prejudice, allowing Hope or other members of the class to refile if their information is ever actually misused. I would, therefore, have affirmed the court below and not addressed the 12(b)(6) motion to dismiss.

SUPREME COURT OF THE UNITED STATES

BARKER & TODD, INC., Petitioner

v.

Anthony HOPE, Respondent

No. 18-251
July 16, 2018

Petitioner's petition for writ of certiorari to the Thirteenth Circuit Court of Appeals is GRANTED limited to the following two questions:

1. Whether Respondent established injury-in-fact to confer standing under Article III;
2. Whether Respondent's state law negligence claims may be based on violations of the Health Insurance Portability and Accountability Act.

IT IS SO ORDERED.