Strautins v. Trustwave Corporation Doc. 50

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

AMBER J. STRAUTINS, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	**No. 12 C 09115**
v.	)	**Judge John J. Tharp, Jr.**
TRUSTWAVE HOLDINGS, INC.,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

In late 2012, a hacker launched a cyber-attack on the South Carolina Department of Revenue ("SCDOR"). In their initial disclosure of the attack, state officials announced that approximately 3.6 million Social Security numbers, 387,000 credit and debit card numbers, and tax records for 657,000 businesses had been exposed. Media reports called it potentially "the largest cyber-attack ever on a state government," putting "other states on high alert."[1]

Before the Court is a class action suit asserting claims arising from this cyber-attack. The plaintiff, Amber Strautins, has sued Trustwave Holdings, Inc. ("Trustwave"),[2] a Chicago-based data security company. According to its website, Trustwave "helps businesses fight cybercrime, protect data and reduce security risk."[3] One of Trustwave's clients is the SCDOR. Strautins

[1] Robbie Brown, *Hacking of Tax Records Has Put States on Guard*, N.Y. TIMES, Nov. 5, 2012, at A17; Robbie Brown, *South Carolina: State Computer System is Hacked*, N.Y. TIMES, Oct. 26, 2012, at A16.

[2] Strautins originally sued Trustwave Corporation. *See* Dkt. 1. She later amended her complaint to replace Trustwave Corporation with Trustwave Holdings, Inc. *See* Plaintiff's Amended Complaint (Dkt. 20) ("Am. Compl."). Trustwave Corporation dissolved in 2012.

[3] *See* www.trustwave.com/our-story/ (last visited March 10, 2014).

Dockets.Justia.com

alleges that Trustwave inadequately protected her personal identifying information ("PII"), which was kept in the SCDOR's database. Trustwave's Motion to Dismiss Strautins' Amended Class Action Complaint is granted for the reasons discussed below.

I. Background

Strautins filed South Carolina tax returns for calendar years 2007 through 2010. Am. Compl. ¶ 12. It is undisputed that in August and September 2012, a hacker cyber-attacked the SCDOR. Am. Compl. ¶¶ 14, 16, 17; Def.'s Mot. to Dismiss (Dkt. 30) ("Def.'s Mot.) at 2-3. The parties offer competing versions of how the attacks occurred, but for the most part the disputes are not material to Trustwave's challenges to the complaint and can be briefly summarized. Strautins alleges that hackers gained access to SCDOR data through "an exposed portal" on the SCDOR website. Am. Compl. ¶¶ 16-17. She further alleges that the hackers "stole and compromised" her PII and that of a putative class comprising of taxpayers who have filed South Carolina tax returns since 1998. Am. Compl. ¶¶ 3, 33.

Trustwave acknowledges that it has provided, and continues to provide, products and services to the SCDOR. Def.'s Mot. at 2. It argues, however, that the data breach was not accomplished through an "exposed portal" on SCDOR's website "or other external vulnerability," but rather was accomplished with authorized user credentials obtained from a "phishing" email sent to, and apparently opened by, a SCDOR employee. *Id.* at 3-4. More significantly, with respect to the issues presented by its motion, Trustwave takes issue with Strautins' claim that all of the data potentially exposed during the attacks was actually "stolen and compromised," arguing that the complaint lacks allegations to support that conclusion, asserting that most of the credit card numbers affected were encrypted, and pointing to media reports suggesting that only tax data of electronic filers was exposed. *Id.* at 4. Unlike the

question of how the attack occurred, the dispute over what actually occurred during the attack matters to the disposition of the defendant's motion and is discussed in greater detail below.[4]

After discovery and disclosure of the cyber-attack, SCDOR announced that it would provide notice to taxpayers whose PII may have been disclosed during the attack.[5] In the meantime, the state set up a website and toll-free hotline for taxpayers to determine if their data was compromised.[6] South Carolina also offered free credit monitoring and protection services, identity-theft insurance, and lifetime credit-fraud resolution to affected individuals.[7] Trustwave emphasizes that Strautins admits that she has not received notice that her data was compromised and that she does not allege that she has used the website or hotline to confirm whether her PII was compromised in the breach. Am. Compl. ¶ 12 ("To date, Plaintiff Strautins has not received formal notification from either Trustwave or SCDOR regarding the Data Breach."); Def.'s Mot. at 5.

---

[4] The complaint does not detail whether Strautins filed paper returns or filed her returns electronically. This fact could have significance to the merits of the dispute because some reports indicate that only tax data supplied in connection with returns filed electronically were exposed during the attack. *See* Andrew Shain, *SC working on security, notifying victims of data breach*, THE STATE, Jan. 6, 2013, www.thestate.com/2013/01/06/2578924/the-latest-on-sc-hacking-costs.html (last visited Mar. 10, 2014).

[5] *See* Andrew Shain, *SC working on security, notifying victims of data breach*, THE STATE, Jan. 6, 2013, www.thestate.com/2013/01/06/2578924/the-latest-on-sc-hacking-costs.html (last visited Mar. 10, 2014) (reporting that the state began sending notification letters in December 2012, that "more than 600,000 of 2.6 million S.C. residents affected have received notifications," that "more than 760,000 of 1.2 million out-of-state residents affected have received notices," and that "notifications should finish in the next few weeks").

[6] *See* Press Release, *SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identify Theft Protection to Taxpayers*, S.C. Dep't of Revenue, Oct. 26, 2012, www.sctax.org/NR/rdonlyres/5AF6995A-F9F0-42E7-A430-EC620CCE8C7D/0/1DORmediarelease.pdf (last visited Mar. 10, 2014).

[7] *See Frequently Asked Questions Regarding SC DOR Security Breach*, S.C. Dep't of Revenue, Nov. 2, 2012, www.sctax.org/NR/rdonlyres/57F3E754-6035-44E1-AF6D-E44BEA94485E/0/FAQ11_2.pdf (last visited Mar. 10, 2014).

Strautins accuses Trustwave of "fail[ing] to adequately safeguard, protect and monitor SCDOR's computer systems" and of "fail[ing] to discover and timely report" the data breach "even though it allegedly scanned SCDOR's computer systems on September 14, 2012, and on October 14, 2012." Am. Compl. ¶¶ 25-26. She maintains that Trustwave's actions "and/or inaction" as well as the data breach have placed the other class members and her at an "imminent, immediate and continuing increased risk of identity theft and identity fraud," and that they "will now be required to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives …." *Id.* ¶¶ 7, 33. On behalf of a putative class comprising "all individuals and businesses who filed … a South Carolina tax return for any year from 1998 through and including 2011," *id.* ¶ 44, Strautins asserts claims against Trustwave for: (1) willful violation of the Fair Credit Reporting Act (Count I); (2) negligent violation of the Fair Credit Reporting Act (Count II); (3) negligence (Count III); (4) invasion of privacy by public disclosure of private facts (Count IV); and (5) breach of contract – third party beneficiary (Count V). *Id.* ¶¶ 55-88.

Trustwave moves to dismiss Strautins' First Amended Complaint for lack of standing pursuant to Federal Rule of Civil Procedure 12(b)(1). Alternatively, it moves for dismissal pursuant to Rule 12(b)(1) for failure to state a claim.

II. Analysis

"In essence the question of standing is whether [Strautins] is entitled to have the court decide the merits of the dispute or particular issues." *See Apex Digital, Inc. v. Sears, Roebuck & Co.*, 572 F.3d 440, 443 (7th Cir. 2009) (citations and quotations omitted). It is Strautins' burden to show that the requirements of standing have been met. *See Kathrein v. City of Evanston*, 636 F.3d 906, 914 (7th Cir. 2011) (citation omitted). All material allegations of Strautins' First

Amended Complaint must be construed as true, and all reasonable inferences are drawn in her favor. *See Reid L. v. Ill. St. Bd. of Educ.*, 358 F.3d 511, 515 (7th Cir. 2004).

To establish standing, Strautins must show: (1) that she suffered an injury in fact; (2) that the injury is fairly traceable to Trustwave's actions; and (3) that the injury will likely be redressed with a favorable decision. *See Kathrein*, 636 F.3d at 914 (citation and quotations omitted). As the Supreme Court recently explained in *Clapper v. Amnesty International*, to convey standing, the injury alleged "must 'be concrete, particularized, and actual or imminent ….'" *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (quoting *Monsanto Co. v. Geerston Seed Farms*, 130 S. Ct. 2743, 2752 (2010)). The Court added, "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending." *Id.* (emphasis in original) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 565 n.2 (1992)). "[A]llegations of *possible* future injury are not sufficient." *Id.* (emphasis in original) (citations and quotations omitted) (holding that there was no Article III standing where chain of speculative possibilities did not establish that injury based on potential future action was "certainly impending").

Strautins claims that she has standing to bring this lawsuit "because she was damaged as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach." Am. Compl. ¶ 6. More specifically, Strautins claims that she and other class members have incurred the following injuries: (1) untimely and/or inadequate notification of the Data Breach; (2) improper disclosure of PII; (3) loss of privacy; (4) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (5) the value of time spent mitigating identity theft and/or identity fraud

and/or the increased risk of identity theft and/or identity fraud; (6) deprivation of the value of PII; and (7) violations of rights under the Fair Credit Reporting Act. *Id.* ¶ 90. These claims of injury, however, are too speculative to permit the complaint to go forward. To the extent that they are premised on the mere possibility that her PII was stolen and compromised, and a concomitant increase in the risk that she will become a victim of identity theft, Strautins' claim is too speculative to confer Article III standing. And even if that were not so (and concededly, as discussed below, the issue is not beyond doubt), the Court would nevertheless conclude that the complaint fails to state a claim because it does not plausibly establish that Strautins' PII was in fact "stolen and compromised" and so is too speculative to state a plausible claim for relief. Whether viewed as a matter of standing or pleading, the allegations set forth in the plaintiff's present iteration of her complaint do not suffice to permit further adjudication of her claims.

A. Standing

Strautins first claims that she and the other class members were injured by the untimely and/or inadequate notification of the Data Breach by the SCDOR. Am. Compl. ¶ 90. Strautins claims that while the breach occurred in late August and early September, Trustwave did not discover the breach until mid-October of 2012, and consequently SCDOR did not disclose the breach to the public until October 26, 2012. *Id.* ¶¶ 3, 18. Strautins implies, although the argument is a bit unclear, that the delayed and/or inadequate notice regarding the breach caused an "imminent, immediate, and continuing increased risk of identity theft and identity fraud," *id*. ¶¶ 3, 7, and therefore suffices to confer standing.

As explained in *Clapper*, however, "allegations of *possible* future injury are not sufficient" to establish standing. 133 S. Ct. at 1147 (emphasis in original). While acknowledging

that "imminence is concededly a somewhat elastic concept,[8] the Court reemphasized its statements in prior cases that to confer standing the threatened injury must be "*certainly impending*." *Id.* at 1147, 1160 (emphasis in original). Employing that standard, the Court held that the threat of government interception of private communications between the plaintiffs and foreign contacts suspected of terrorism was too speculative to confer standing on the plaintiffs to challenge the law authorizing government surveillance of "non-United States persons" because realization of the harm alleged—the interception of the plaintiffs' communications with such persons—was dependent on a variety of events and actions by independent third parties that might never come to pass. 133 S. Ct. at 1148-50.

Clapper compels rejection of Strautins' claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing. *See, e.g.*, *In Re Barnes & Noble Pin Pad Litig.*, No. 12 C 08617, 2013 WL 4759588, at *2 (N.D. Ill. Sept. 3, 2013) (granting motion to dismiss for lack of standing in part because the plaintiffs did not show an injury that was "certainly impending" under *Clapper*); *Galria v. Nationwide Mut. Ins. Co.*, No. 13 C 118, 13 C 257, 2014 WL 689703, at *6 (S.D. Ohio Feb. 10, 2014) (same); *Hammer v. Sam's East, Inc.*, No. 12 C 2618, 2013 WL 3756573, at *3 (D. Kan. July 16, 2013) (same). Whether Strautins or other class members actually become victims of identity theft as a result of the data breach depends on a number of variables, such as whether their data was actually taken during the breach, whether it was subsequently sold or otherwise transferred, whether anyone who obtained the data attempted to use it, and whether or not they succeeded. Strautins' complaint, filed less

[8] The Court acknowledged that its "cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm … [But] plaintiffs bear the burden of pleading and proving concrete facts showing that the defendant's actual action has caused the substantial risk of harm." *Id.* at 1150 n.5.

than three weeks after the data breach was first announced by the SCDOR, provides no basis to believe that any of these events have come to pass or are imminent. Like the plaintiffs in *Clapper*, the harm that Strautins fears is contingent on a chain of attenuated hypothetical events and actions by third parties independent of the defendant. 133 S. Ct. at 1148. Although Strautins does not need to show that it is "literally certain" that she will be a victim of identity theft and/or fraud, she has not alleged facts that would plausibly establish an "imminent" or "certainly impending" risk that she will be victimized. Under *Clapper*, the mere fact that the risk has been increased does not suffice to establish standing.[9]

Strautins' allegations are insufficient to show that she and others face a "certainly impending" risk of identity theft and her own complaint makes the point. In her complaint, Strautins cites a "2012 Identity Fraud Report" issued by Javelin Strategy & Research (which she describes as "a leading provider of quantitative and qualitative research") which found that "individuals whose PII is subject to a reported data breach ... are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft." Am. Compl. ¶ 7. The plaintiff does nothing more to quantify the risk she now faces, which makes it impossible to assess the import of this risk factor; this statistic only confirms that many people whose PII are

[9] *Clapper* similarly requires rejection of Strautins' claim of standing based on her allegations that she and the other class members will be forced to incur out-of-pocket expenses to mitigate an increased risk of identity theft and/or fraud. Strautins lists some of these potential expenses in her complaint: changing PIN numbers on payment cards, placing freezes and alerts with credit reporting agencies, closing or modifying financial accounts, and closely reviewing and monitoring those accounts. Am. Compl. ¶ 33. She adds that on average, "[v]ictims and potential victims of identity theft and identity fraud" incur $1,513 in economic loss and $354 in out-of-pocket expenses. *Id.* ¶ 34. *Clapper* made clear that such expenses do not confer standing, holding that plaintiffs "cannot manufacture standing by incurring costs in anticipation of non-imminent harm." 133 S. Ct. at 1155. Strautins does not allege that she has already incurred costs, but even if she had, her fear that these costs would come to bear would be insufficient to establish standing. *See also, e.g., Polanco v. Omnicell, Inc.*, No. 13 C 1417, 2013 WL 6823265, at *14 (D.N.J. Dec. 26, 2013) (rejecting plaintiff's incurred costs as sufficient to demonstrate standing).

exposed in a data breach do not become victims of identity theft. If the risk of identity theft absent a data breach is minimal, multiplying it by 9.5 will not elevate that risk to "certainly impending" status. If the general risk of identity theft is 2.5%, for example, that would suggest that less than one in four people who are exposed to a data breach would be victimized (.025 x 9.5 = .2375, or 23.75%). And for purposes of further illustrating the point (rather than endorsing the statistic), the Court also notes that on its web site, Javelin reports that in 2012, one in four people who received a data breach notification became a victim of identity theft—which, if accurate, means that 75% of even those most likely to be victimized by identity theft (*i.e.*, those who were exposed to a data breach)—are not. *See* http://www.marketwatch.com/story/fraud-hits-one-in-three-data-breach-victims-2014-02-05 (last visited Mar. 10, 2014). *See also Galria*, 2014 WL 689703, at *5 (plaintiff's data showing "that consumers who receive a data breach notification had a fraud incidence rate of 19% in 2011" demonstrate that harm is not "certainly impending"). The point is not that those whose PII are exposed in a data breach are not at greater risk of identity theft; the point is that Strautins has failed to meet her burden to establish that identity theft is "certainly impending" for South Carolina taxpayers like herself.

Strautins maintains that, notwithstanding *Clapper*, the Seventh Circuit's opinion in *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007) controls the standing inquiry in this case. In *Pisciotta*, the Seventh Circuit held that it had jurisdiction to adjudicate claims arising from the hacking of confidential information consumers had submitted through the defendant bank's on-line application process. *Id.* at 634. Noting that the plaintiffs alleged neither that they had been victims of identity theft nor that they had incurred any direct financial loss as a result of the breach, the Court of Appeals nevertheless held that "a threat of future harm or …an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have

otherwise faced, absent the defendant's actions," satisfied the injury-in-fact requirement for Article III standing. *Id.* In so holding, the *Pisciotta* court did not discuss the requirement that a threat of harm be "imminent" or "certainly impending" (again, standards that *Clapper* reemphasized but did not invent), and posited no bar at all to the use of probabilistic harm as a basis for standing; the opinion contains no language describing the degree of risk exposure required to confer standing and leaves open by implication the argument that *any* degree of risk enhancement could suffice. *See id.* at 633-34. And, indeed, that was arguably the prevailing view in this Circuit before *Clapper*. In *Elk Grove Village v. Evans*, for example, the Seventh Circuit stated, in rejecting a standing challenge premised on the possibility that future flooding in Elk Grove Village would be exacerbated by the defendant's construction of platforms for cellular antenna towers, that the Village's "injury is of course probabilistic, but even a small probability of injury is sufficient to create a case or controversy …." 997 F.2d 328, 329 (7th Cir. 1993).

Clapper does not completely close the door on probabilistic harm as a basis for standing—harm that is "imminent" or "certainly impending" is, by definition, harm that has not occurred. *See Brandt v. Village of Winnetka*, 612 F.3d 647, 649 (7th Cir. 2010) ("Injury need not be certain. Any pre-enforcement suit entails some element of chance …."). Nevertheless, the import of the Supreme Court's decision in *Clapper* is that, whatever verbal formulation is used to describe it, the threshold of probability for injuries that have not actually occurred is high. While acknowledging that literal certainty is not required, *Clapper* seems rather plainly to reject the premise, implicit in *Pisciotta* and fairly explicit in *Elk Grove Village*, that *any* marginal increase in risk is sufficient to confer standing. Indeed, *Clapper* expressly rejected the Second Circuit's "objectively reasonable likelihood" standard as "inconsistent with our requirement that threatened injury must be certainly impending to constitute injury in fact." *See* 133 S. Ct. at

1147-48 (internal quotation omitted). It is difficult, to say the least, to reconcile that specific holding, and the Court's emphatic reiteration of the "certainly impending" standard, with the Seventh Circuit's seeming view in *Pisciotta* that any risk of future harm suffices to confer standing.[10]

Strautins defends *Pisciotta*'s continuing viability only by arguing (in a single sentence) that because *Clapper* did not purport to change Article III standing law, *Pisciotta* must remain in force. Whether *Clapper* changed the law or merely clarified it, however, this Court is required to attempt to apply its teachings faithfully.[11] If existing circuit precedent cannot be reconciled with a subsequent ruling from the Supreme Court, then the latter governs. All Article III courts "are bound to follow the holdings of our Nation's highest court …." *Robb v. Norfolk & Western Ry. Co.*, 122 F.3d 354, 361 n.5 (7th Cir. 1997). "If there [is] a conflict between this circuit's precedent and Supreme Court precedent, we are bound to follow the Supreme Court." *Id.* (quoting *Bae v. Peters*, 950 F.2d 469, 478 (7th Cir. 1991)). *See also, e.g., Cameo Convalescent Ctr., Inc. v. Percy*, 800 F.2d 108, 110 (7th Cir. 1986) (district court properly disregarded Circuit

[10] Trustwave argues that *Pisciotta* is distinguishable because in that case the plaintiffs' data actually had been accessed by the hackers. Def.'s Reply (Dkt. 36) at 2. So far as this Court can discern, however, nowhere in the opinion did the *Pisciotta* court indicate whether the plaintiffs' data had actually been obtained as a result of the data breach or whether they were simply concerned about the possibility that it had been stolen. Accordingly, the opinion cannot, in the Court's view, be distinguished on that basis.

[11] It may be a stretch to say that Clapper "clarified" standing law, given the breadth and variety of standing cases, the myriad formulations that courts have used to articulate when injury is sufficiently likely to confer standing, the Court's own recognition that it had applied less rigorous standards in some contexts, and its acknowledgment that the Court has traditionally scrutinized standing claims most closely when reviewing challenges to actions by the Executive or Legislative branches of government, 133 S. Ct. at 1147. Thus, in this Court's view, the question of whether the risk of identity theft confers standing on Strautins, and the import of *Clapper* for standing analysis in the Seventh Circuit, is a question on which reasonable minds may differ. Ultimately, however, as discussed further below, the issue is not controlling here because Strautins has failed even to plausibly allege that her PII was stolen and so she has failed to establish even the proposition that she is at an increased risk of identity theft as a result of the SCDOR data breach.

precedent in light of intervening opinion by Supreme Court changing the law); *Lee v. United States,* 570 F. Supp. 2d 142, 149-50 (D.D.C. 2008) ("when holdings of the Supreme Court and the D.C. Circuit are irreconcilable, the Supreme Court's decision will trump every time"). In the wake of the Court's emphatic reiteration in *Clapper* of the "certainly impending" standard for assessing the sufficiency of probabilistic harm to confer standing, the absence of any suggestion by the Court that this standard does not apply generally to standing analysis, and the similarity of the factual contexts between *Clapper* and this case (both involving the potential unauthorized disclosure of sensitive personal information), this Court concludes that it is duty bound to apply that standard in this case notwithstanding seemingly inconsistent Seventh Circuit precedent that predates *Clapper*.[12] To the extent that *Pisciotta* stands for the proposition that a risk of future harm does not have to be "imminent," "certainly impending," or pose greater than an objectively reasonable likelihood of injury (the standard *Clapper* expressly rejected as inadequate), this Court cannot square it with *Clapper*.

Clapper was decided after the principal briefs in this matter had been submitted. Strautins' principal response to *Clapper* is retreat. Rather than continue to argue that the speculative risk of identity theft provides standing, she notes that she has alleged "far more than the increased risk of identity theft or identity fraud as the basis for her damages." Dkt. 42 at 3. Specifically, Strautins maintains that because her PII was "stolen and compromised" during the attack, she has already been directly injured in a number of ways, such as her loss of privacy and loss of the ability to sell her PII. *Id.* Because those claims rest on the adequacy of her claim that her data were, in fact, stolen and compromised, the Court turns next to that issue.

[12] In *Barnes & Noble*, 2013 WL 4759588 (N.D. Ill.), the court relied on *Clapper* in dismissing a motion to dismiss for lack of standing in a data breach case without reference to *Pisciotta*.

B. Data Compromise Allegations

Strautins maintains that Trustwave's actions "caused a substantial unauthorized disclosure of Plaintiff's and the other Class Members' PII." Am. Compl. ¶ 5. As this is a motion to dismiss, Strautins is of course entitled to the reasonable inferences that may be drawn from her complaint. *See Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009). That said, the Court need not accept as true statements of law or unsupported conclusory factual allegations. *See McCauley v. City of Chicago,* 671 F.3d 611, 616 (7th Cir. 2011). To survive a motion to dismiss, the complaint must "state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal,* 556 U.S. at 678. "Where a complaint pleads facts that are 'merely consistent with' a defendant's liability, it 'stops short of the line between possibility and plausibility of entitlement to relief.'" *Id.* (quoting *Twombly,* 550 U.S. at 557). "In such a case, the inference of liability is merely speculative." *Yeftich v. Navistar, Inc.*, 722 F.3d 911, 915 (7th Cir. 2013). "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'shown'—'that the pleader is entitled to relief.'" *Iqbal,* 556 U.S. at 679 (quoting FED. R. CIV. P. 8(a)(2)).

Strautins alleges that her PII was "stolen and compromised," Am. Compl. ¶ 3, as a result of the breach of the SCDOR database, but that is a conclusion in need of factual support. Her complaint rests entirely on the assumption that her PII was disclosed because (1) the SCDOR was cyber-attacked and (2) because she filed tax returns in South Carolina. But the fact that hackers gained some access to a SCDOR database does not necessarily mean, or even plausibly

suggest, that they obtained access to all of the data in SCDOR's possession, and the complaint provides no basis to infer that the hacker (or hackers) obtained *her* data.

Strautins points to the SCDOR's press release announcing the data breach as the support for her claim that her data was compromised. In her response brief, she states that "[a]ccording to SCDOR, the Data Breach affected all individuals and businesses that filed, or on whose behalf was filed, a South Carolina tax return for any year from 1998 through and including 2011." Dkt. 35 at 8. She adds, "[A]s the SCDOR website makes clear, any individual who has filed a South Carolina tax return since 1998 is affected." *Id.* at 8-9. To read Strautins' brief, one would believe that the SCDOR announced that data of all tax filers between 1998 and 2012 had been compromised (and since she was a tax filer, her PII must have been affected too).

But this is not so. The SCDOR makes clear on its website and in its announcements that certain tax filers' PII ***may*** have been affected, or had been ***potentially*** compromised, by the breach.[13] The October 26, 2012, news release posted to the SCDOR website states, "The S.C. Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been ***exposed*** in a cyber attack."[14] The release continues,

> Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1-866-578-5422 to determine ***if their information is affected. If so,*** the taxpayer can immediately enroll in one year of identity protection service provided by Experian.[15]

[13] In view of Strautins reliance on the SCDOR's pronouncements via its website, the Court may refer to the contents of this website, which is referenced in the complaint and central to the plaintiff's allegations. *See Venture Assocs. Corp. v. Zenith Data Syst. Corp.*, 987 F.2d 429, 431 (7th Cir. 1993). The Court has added the emphasis in this and the subsequent quotes to focus on language showing that Strautins' characterization of the SCDOR's statements is not accurate.

[14] *See* http://www.sctax.org/News+Releases/20121009_1026NR.htm (last visited Mar. 10, 2014) (emphasis added).

[15] *Id.* (emphasis added).

The SCDOR offered the one year of free CSID identity protection services to individuals and businesses "whose information was *potentially* compromised in the security breach …" and who "*may* be eligible" if they filed an electronic South Carolina tax return between 1998 and 2012.[16] The SCDOR further announced:

> If you filed a South Carolina tax return since 1998, you are urged to call the toll-free call center that DOR has established, which will be operating 24/7 beginning at noon on Friday, October 26, 2012, for anyone who wishes to know ***if*** their personal information was included …[17]

Plainly, the data breach did *not* result in the compromise of data of all taxpayers filing South Carolina returns since 1998 (or, to be more accurate, plainly the SCDOR announcement, on which Strautins relies as the sole support for her claim that her data were compromised, does not support such an inference). Were that the case, there would have been no need to provide a hotline for taxpayers to call to determine whether their data had been exposed. The SCDOR website makes clear that some tax filers may have been affected while others were not, and Strautins' complaint lacks any allegations to plausibly place her into the former group rather than the latter. At most, then, her allegations are "consistent with" the possibility that her data were stolen, but, again, where a complaint pleads facts that are "merely consistent with" a defendant's liability, it "stops short of the line between possibility and plausibility of entitlement to relief."[18] *Iqbal*, 556 U.S. at 678.

---

[16] *See* www.sctax.org/security (last visited Mar. 10, 2014) (emphasis added).

[17] *See* http://www.sctax.org/NR/rdonlyres/3961B679-C036-4722-A475-473407A8B1D6/0/2Chronology.pdf (last visited Mar. 10, 2014) (emphasis added).

[18] The Court notes as well that in her complaint, Strautins concedes that she has not sought or received any notice from the SCDOR that her PII was compromised by the breach. Am. Compl. ¶ 12 ("To date, Plaintiff Strautins has not received formal notification from either Trustwave or SCDOR regarding the Data Breach."). Thus, her claim that her own data were stolen may not even be "consistent with" the facts she has set forth.

Accordingly, the complaint fails plausibly to allege that Strautins' PII was stolen and compromised and thus fails in this way too to establish standing to pursue any of her claims. Further, because each of the plaintiff's legal claims are predicated on her inadequate allegations that her data were stolen and compromised,[19] the Court would dismiss them for failure to state a claim even if her allegations of potential harm sufficed for purposes of standing. Notwithstanding the issue of standing, then, this shortcoming would result in the dismissal of the plaintiff's Fair Credit Reporting Act, Invasion of Privacy, negligence, and breach of contract claims.

Finally, a word concerning the plaintiff's assertion of claims against Trustwave under the Fair Credit Reporting Act. Strautins alleges that she and the other class members "suffered (and continue to suffer) damages in the form of … rights they possess under FCRA—for which they are entitled to compensation" and statutory damages. Am. Compl. ¶ 90. As an initial matter, "rights" are not a type of injury by itself, and an allegation that a defendant violated a statute is not sufficient to confer standing; the plaintiff must also allege that she has been injured by the violation to establish standing. *See FMC Corp. v. Boesky*, 852 F.2d 981, 998 (7th Cir. 1988). The complaint fails to do so.

Even more fundamentally, the FCRA governs only the conduct of "consumer reporting agencies."[20] As such, it seems to have no application to Trustwave, which so far as the Court can

---

[19] Each of the plaintiff's legal theories (asserting violation of the Fair Credit Reporting Act, invasion of privacy, negligence, and breach of contract) requires the plaintiff to establish that her data were "stolen and compromised." *See* Am. Compl. ¶¶ 60, 62, 66, 68, 75, 86.

[20] "Consumer reporting agency" is defined as

> any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing

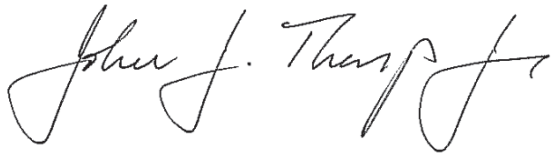
tell from the plaintiff's allegations does not "engage[] … in the practice of assembling or evaluating consumer credit information … for the purpose of furnishing consumer reports to third parties." 15 U.S.C. § 1681a(f). Strautins does not maintain that Trustwave has some side business distributing consumer reports; rather, she argues that Trustwave qualifies as a consumer reporting agency because it "assembled" consumer data by virtue of the data security services it provides to its clients and "furnished" that data by means of its negligent or willful failure to safeguard the data. Dkt. 35 at 9-10. Even putting aside the problems with these contentions—*see, e.g.*, *Holmes v. Countrywide Fin. Corp.*, No. 08C 205, 2012 WL 2873892, at *16 (W.D. Ky. July 12, 2012) (plaintiff did not adequately allege that defendant "furnished" financial information to a third party who had engineered "an elaborate and sophisticated theft")—the plaintiff's argument still fails, as Strautins does not allege, and cannot plausibly maintain, that Trustwave's "purpose" was to furnish the information to data thieves. To the contrary, the complaint alleges that Trustwave's purpose was just the opposite—to prevent anyone from getting the information. Am. Compl. ¶ 9 ("SCDOR contracted with Trustwave for the purpose of safeguarding, monitoring, and protecting SCDOR's computer systems."). While the Court will not preclude Strautins from repleading this claim in an amended complaint, her attorneys are advised that the assertion of the claim in the pending complaint raises, in the Court's view, concerns about compliance with the requirements of Rule 11. *See Frederick v. Marquette Nat'l Bank*, 911 F.2d 1, 2 (7th Cir. 1990) (affirming dismissal of suit against bank because bank was not a "credit reporting agency" under the FCRA and "[w]hen a statute expressly confines liability to X's and the defendant is a Y, the suit is frivolous.").

> consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

* * * * *

For the reasons stated above, the Court concludes that Strautins' claimed injuries are insufficient to establish standing for Article III purposes. Alternatively, in the event that the Court's conclusion about Strautins' standing is in error, the Court concludes that her complaint fails to state a claim for relief. Accordingly, the complaint is dismissed without prejudice. Plaintiff is granted leave to replead within 28 days of the entry of this Order.



Entered: March 12, 2014

John J. Tharp, Jr.
United States District Judge