IN THE SUPERIOR COURT OF THE STATE OF DELAWARE
IN AND FOR NEW CASTLE COUNTY

GAIL SLAUGHTER, STEVEN H. AMICK, JACOB HABER, AND KAROL POWERS-CASE, on their behalf and on behalf of those similarly situated,	)	
Plaintiffs,	)	
	)	C.A. No.: 10C-09-001 FSS
v.	)	CCLD
	)	**(E-FILED)**
AON CONSULTING, INC., AON CONSULTING, INC. OF NEW JERSEY, AON CONSULTING WORLDWIDE, INC., AON CORPORATION,	)	
Defendants.	)	

Submitted: November 21, 2011
Decided: January 31, 2012

ORDER

Upon Defendants' Motion to Dismiss – *GRANTED.*

Through Defendants' alleged negligence, approximately 22,000 State of Delaware retirees' personal information was placed on a public website, and accessed approximately 100 times by servers in China. Plaintiffs, themselves retirees, seek class certification to represent all similarly situated retirees' interests. After one year of discovery limited to determining actual harm, only two retirees have had any identity theft issues. Even so, Plaintiffs have not shown Aon's breach was the cause.

Plaintiffs have obtained an expert report, but it failed to show any actual injuries. Thus, under a consistent line of authorities addressing similar negligence throughout the country, Plaintiffs do not have standing to maintain a claim on their own or on behalf of other retirees, because they have not alleged Defendants' breach actually caused an injury in fact. At best, Plaintiffs have alleged reasonable fear of future possible harm. That, however, does not amount to actionable injury, as the law stands now.

I.

As mentioned, Plaintiffs are retired state employees. Aon, collectively, are benefits consulting firms hired by Delaware's retirement system. Aon compiled retiree information to facilitate bids from insurers interested in providing vision health coverage. The information package contained the retirees' Social Security numbers, birth dates, and genders, but did not contain their individual names.

Aon submitted the unencrypted information to the State benefits office, confirming it was ready for posting. The State posted the information on its publically accessible procurement site on August 16, 2010. The breach was detected and removed from the site on August 20, 2010.

Aon admits it did not randomize the information to prevent identification. In response to its mistake, Aon offered affected retirees $25,000 in

identity theft coverage and free credit monitoring for one year, at Aon's expense. After discussion with the State, Aon increased its monitoring offer to three years.

On September 22, 2010, Plaintiffs filed a complaint on all affected retirees' behalf, alleging Aon: negligently breached its contract to protect sensitive information; and violated 11 *Del. C.* § 935 and 6 *Del. C.* § 2511.

On October 22, 2010, Aon moved to dismiss. The court denied Aon's motion, granting Plaintiffs limited discovery to prove actual harm or submit an expert report showing probability of injury caused by the data breach.[1] On September 23, 2011, after the focused discovery concluded, Aon again moved to dismiss, claiming Plaintiffs still have not shown actual harm. On October 31, 2011, the court heard oral argument, and transcripts were filed on November 21, 2011.

II.

In a Rule 12(b)(6) motion to dismiss, the court determines whether Plaintiffs have stated a claim upon which relief can be granted. The court accepts all factual allegations in the complaint and will deny the motion unless Plaintiffs could not recover under any reasonably conceivable circumstances.[2]

---

[1] *See Baker v. Smith & Wesson*, 2002 WL 31741522, at *3 (Del. Super. Nov. 27, 2002) (Silverman, J.) ("The court gave the Mayor and the City an opportunity to present some legally cognizable damages.").

[2] *Spence v. Funk,* 396 A.2d 967, 968 (Del. 1978).

Delaware courts require plaintiffs to have standing when filing a claim.[3] Standing is a "necessary threshold inquiry a court must undertake before hearing a claim for relief."[4] To establish standing, plaintiffs must show they have suffered an actual, not hypothetical, injury.[5] As discussed below, the focused discovery does not undermine the holding that the complaint fails to state a claim due to its failure to allege compensable injury.

III.

As mentioned, Plaintiffs obtained an expert. The court warned, however:

> I cannot emphasize more strongly how unhelpful it will be to get a superficial affidavit from a so-called expert or even a legitimate expert to say in general terms that what has happened to the plaintiffs here is a bad thing. The standard here is that the named plaintiffs . . . stand personally to lose X percent chance of economic loss, and X ought to be more than fifty percent to show that they probably are going to suffer some harm."[6]

Cyber-security specialist Patrick Stump submitted a report detailing

---

[3] *Dover Hist. Soc'y v. City of Dover Planning Comm'n,* 838 A.2d 1103, 1109 (Del. 2003).

[4] *Id.* at 1110.

[5] *Id.* (quoting *Soc'y Hill Towers Owners' Ass'n v. Rendell*, 210 F.3d 168, 175-76 (3d Cir. 2000)).

[6] *See* Mot. to Dismiss Hr'g Tr. 67:6-11, 67:19-68:2, Dec. 6, 2010.

nationwide credit card theft trends, the potentially catastrophic effect of data breaches, and Chinese hacking methods. While Stump raises reasons for concern, his report never states Aon's breach caused Plaintiffs' actual harm, nor does it show there is a probability that harm will occur.

No named plaintiff has suffered an actual, demonstrated injury. Only two, unnamed retirees have had incidents that might be identity theft: one had a cell phone opened in his name, and the other had credit cards opened in her name. There is no evidence, however, that these incidents were probably caused by Aon's alleged breach, as opposed to the overall risk of identity theft that everyone faces. There is no reason to believe the two incidents were not the result of something else. Stump, himself, agrees identity theft is a widespread problem.

Specifically, Stump states, "It is this expert's opinion that the more than 22,000 state retirees whose data was placed online for four days are - if not assured that they will be targeted for identity theft - at an exceedingly high risk for such theft." He also states, "In sum, if the victims of Aon's data breach are indeed targeted by identity thieves, the results can range from severe to catastrophic and face a significantly heightened risk of identity theft." Again, Stump fails to mention either actual harm or a percentage chance that harm is likely to result.

Stump concludes, "I believe that the data is in the hands of the identity

thieves and will be exploited as soon as it is commercially reasonable to do so - as soon as the identity theft ends." In other words, Stump concludes that identity theft is potentially very harmful and what Aon did increases the risk of it for Plaintiffs.

Stump's opinions are conclusory and speculative and do not merit an elaborate *Daubert*[7] analysis. Assuming that he is a qualified expert, Stump's opinions are not helpful in understanding the evidence or determining a fact in issue.[8] Stump's opinion "did not identify any percentage deviation from the 'norm' or a recurring error rate to compensate for the out-of-the-ordinary person."[9] Thus, not only is his superficial opinion unhelpful, it is potentially confusing or unfairly prejudicial.[10]

IV.

This situation - negligent release of personal identifying information - may be new to Delaware. Other courts have "dismissed similar claims, most brought as purported class actions, in which plaintiffs seek damages for the loss of personal identification information through accident or theft."[11]

---

[7] *Daubert v. Merrell Dow Pharmaceuticals, Inc.,* 509 U.S. 579 (1993). *See also M.G. Bancorporation, Inc. v. Le Beau,* 737 A.2d 513, 522 (Del. 1999) ("We hereby adopt the holding[] of *Daubert*.").

[8] D.R.E. 702.

[9] *Eskin v. Carden,* 842 A.2d 1222, 1231 (Del. 2004).

[10] *See id.* (Upholding expert testimony's exclusion because its prejudice outweighed its relevance).

[11] *Hammond v. The Bank of New York Mellon Corp.*, 2010 WL 2643307, at *1 (S.D.N.Y. June 25, 2010).

For example, in *Allison v. Aetna, Inc.*, a plaintiff placed personal information on Aetna's job application website.[12] Several months later, he started receiving "phishing" emails, purportedly from Aetna, requesting additional personal information.[13] Aetna admitted that its database, containing around 450,000 applicants' names, birthdates, Social Security numbers, e-mail addresses, and other data, was breached, and listed individuals received spam e-mail.[14] *Allison* concludes, "Plaintiff's alleged injury of an increased risk of identity theft is far too speculative based on the factual allegations in this case. Therefore, Plaintiff lacks standing."[15]

Two analogous New Jersey district court cases have dismissed claims because the plaintiffs lacked standing. *Hinton v. Heartland Payment Systems, Inc.* dismissed because the plaintiff "fail[ed] to assert that a third party has actually used his credit information to either open a credit card account or otherwise secure a fraudulent benefit at his expense, and merely speculat[ed] as to a loss of wages or business income."[16]

---

[12] *Alison v. Aetna,* 2010 WL 3719243, at *1 (E.D. Pa. Mar. 9, 2010).

[13] *Id.*

[14] *Id.* at *5-6.

[15] *Id.* at *6.

[16] *Hinton v. Heartland Payment Systems, Inc.,* 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009).

Giordano v. Wachvoia Sec., LLC also dismissed a similar claim.[17] Plaintiff opened an individual retirement account with Wachovia and provided personal information. Approximately ten months later, Wachovia printed 10,000 customers' information to ship to a regional branch. The package never reached its destination.[18] Plaintiff sued, alleging negligence and demanding, "Wachovia establish a credit monitoring program, at Wachovia's expense, 'to ensure timely detection of any and all persons who attempt to use Plaintiff's information as a result of the carelessness and reckless conduct of [Wachovia]' or that Wachovia reimburse Plaintiff for such services."[19]

The court dismissed because "Plaintiff's allegations that, as a result of Wachovia's actions, she will incur costs associated with obtaining credit monitoring services in order to prevent identity theft simply does not rise to the level of creating a concrete and particularized injury. Plaintiff's claims, at best, are speculative and hypothetical future injuries."[20]

This dismissal trend is nationwide. In *Cooney v. Chi. Pub. Schs.,* the Chicago Board of Education hired a printing company to create a COBRA insurance

---

[17] *Giordano v. Wachovia Sec., LLC,* 2006 WL 2177036 (D.N.J. July 31, 2006).

[18] *Id.* at *1.

[19] *Id.* at *2.

[20] *Id.* at *4.

information packet for Chicago Public School employees.[21] The printing company accidentally sent each employee a packet containing 1700 public school employees' personal identifying information, including names, addresses, and Social Security numbers.[22] The plaintiffs "allege[] actual damages because the disclosure put them at increased risk of future identity theft."[23] *Cooney* upheld dismissal because "without actual injury or damage, the plaintiffs' claims 'constitute[d] conjecture and speculation.'"[24]

Paul v. Providence Health Sys.-Or. upheld a similar dismissal.[25] Plaintiffs claimed defendant had negligently failed to safeguard and encrypt data after an estimated 350,000 patients' unencrypted personal, medical, and financial records were stolen from a defendant's employee's car.[26]

Plaintiffs allege that they have been exposed to "past and future out-of-pocket losses associated with placing and maintaining fraud alerts, to credit injuries inherent in credit monitoring and placing and maintaining fraud alerts, and to repair

---

[21] *Cooney v. Chi. Pub. Schs.,* 943 N.E.2d 23, 27 (Ill. App. Ct. 2010), *appeal denied*, 949 N.E.2d 657 (Ill. 2011).

[22] *Id.*

[23] *Id.* at 31.

[24] *Id.* (quoting *Yu v. Int'l Bus. Machines Corp.*, 732 N.E.2d 1173, 1177 (Ill. App. Ct. 2000)).

[25] *Paul v. Providence Health Sys.-Or.,* 240 P.3d 1110 (Or. Ct. App. 2010), *review allowed,* 255 P.3d 489 (Or. 2011).

[26] *Id.* at 1112.

costs of credit damage caused by the theft of data."[27] Dismissing the claim, *Paul* held the plaintiffs had only pleaded economic loss, not actual injury.[28]

In summary, the string of dismissals is unbroken. No court has allowed a similar case to go to trial. The fact that there is a string of cases is troubling. Perhaps, the legislature or the Restatement needs to consider this problem. Meanwhile, the court is unaware of a similar case where a plaintiff has gotten past the dismissal stage.

V.

For the foregoing reasons, Defendants' motion to dismiss is **GRANTED** without prejudice to an injured Plaintiff's filing a timely complaint.[29]

IT IS SO ORDERED.

/s/ Fred S. Silverman
Judge

cc: Prothonotary (Civil)
pc: Bruce L. Hudson, Esquire
Mark M. Billion, Esquire
Jon E. Abramcyzk, Esquire
Matthew R. Clark, Esquire
James E. Brandt, Esquire

---

[27] *Id.*

[28] *Id.* at 1114-15.

[29] *See Riley v. Schnee*, 560 A.2d 491, 1989 WL 47245, at *1 (Del. Mar. 29, 1989) (TABLE) (10 *Del. C.* § 8119 covers personal injury claims originating in tort). *See also Layton v. Allen*, 246 A.2d 794, 797 (Del. 1968) (Discussing inherently unknowable injury).