UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE:

SCIENCE APPLICATIONS INTERNATIONAL CORP. (SAIC) BACKUP TAPE DATA THEFT LITIGATION

Misc. Action No. 12-347 (JEB)

This document relates to:

MDL No. 2360

ALL CASES

MEMORANDUM OPINION

In September 2011, a thief broke into a car sitting in a San Antonio parking garage and stole the car's GPS system, stereo, and several data tapes. This seemingly run-of-the mill theft has spawned massive litigation. Why? Because of the contents of those pilfered tapes. The car, as it turns out, belonged to an employee of Science Applications International Corporation, an information-technology company that handles data for the federal government. And the tapes contained personal information and medical records concerning 4.7 million members of the U.S. military (and their families) who were enrolled in TRICARE health care, which contracts with SAIC – somewhat ironically – to protect patients' data.

Plaintiffs, who are potential victims of the data breach, filed a number of lawsuits in various courts around the country alleging harm from an increased likelihood of identity theft and from an invasion of their privacy, among other things. Eight of those suits have been consolidated here as a multi-district litigation. Recently, SAIC and the three Government Defendants – TRICARE, the Department of Defense, and its Secretary, Chuck Hagel – moved to dismiss the now-consolidated Complaint. Defendants claim that the service members can show

no injury based on the data breach and hence lack standing to sue in federal court; in addition, SAIC and the Government contend, none of the victims has stated a claim for relief under any of the many federal and state laws that might protect them. Plaintiffs rejoin that they have, in fact, been injured by the breach and that their various causes of action – ranging from state tort law to the federal Privacy Act of 1974 – are sound.

This case presents thorny standing issues regarding when, exactly, the loss or theft of something as abstract as data becomes a concrete injury. That is, when is a consumer actually harmed by a data breach – the moment data is lost or stolen, or only after the data has been accessed or used by a third party? As the issue has percolated through various courts, most have agreed that the mere loss of data – without evidence that it has been either viewed or misused – does not constitute an injury sufficient to confer standing. This Court agrees. Mere loss of the data is all that most Plaintiffs allege here, so the majority must be dismissed from this case. Two Plaintiffs, however, do plausibly assert that their data was accessed or abused, and those victims may move forward with their claims.

Standing thus resolved, the Court would typically next delve into the merits of the remaining Plaintiffs' claims. In this case, however, the Court believes it more advisable to pause and confer with the litigants. The dismissal of most Plaintiffs will have serious consequences moving forward, which may well alter the parties' perceptions of the case and how they prefer to proceed. Not every count in the Complaint applies to every Plaintiff, for example – so many of the counts may fall on that basis alone. Given that many of the Plaintiffs have been dismissed, moreover, they may desire to appeal immediately, which the Court might sanction. See Fed. R. Civ. P. 54(b). This matter was, after all, intended to proceed as a class action, and the number of potential class members has now considerably diminished. The Court will thus hold a status

hearing to assess the parties' intentions before taking up the question of whether the two remaining Plaintiffs have stated a legal claim.

I. Background

A. Factual Background

As outlined above, this case revolves around the theft of several data tapes from an SAIC employee's car in 2011. See Compl., ¶¶ 99-100. As the police report indicates, those tapes were taken along with a GPS and stereo when a criminal smashed a window and broke into the vehicle in mid-September. See SAIC Mot., Exh. A (San Antonio Police Report of Sept. 14, 2011) at 2-3; Compl., ¶ 100.[1] Despite the efforts of law enforcement, the thief was never apprehended.

The tapes were backup copies of medical data related to over 4 million TRICARE beneficiaries who had received medical treatment or testing in San Antonio, Texas. See Compl., ¶ 93. On September 29, 2011, TRICARE released a statement detailing the data breach to alert customers to the situation. See id. In November, SAIC mailed letters to affected service members explaining the scope of the theft and noting that "the information contained on the tapes may include names, Social Security Numbers, addresses, dates of birth, phone numbers," and a variety of medical information. SAIC Mot., Exh. B (Letter from SAIC to Customer (Nov. 16, 2011)) at 1; see Compl., ¶ 94.[2] But the tapes did not include "any financial data, such as credit card or bank account information." Letter from SAIC at 1. SAIC also observed, "The chance that [any] information could be obtained from these tapes is low since accessing, viewing and using the data requires specific hardware and software." Id. SAIC nevertheless offered all

[1] The police report is a public record subject to judicial notice. See Kaempe v. Myers, 367 F.3d 958, 965 (D.C. Cir. 2004). In addition, when a court considers jurisdictional arguments, it may rely on evidence outside of the Complaint. See Jerome Stevens Pharms., Inc. v. FDA, 402 F.3d 1249, 1253 (D.C. Cir. 2005).

[2] The Letter from SAIC is incorporated by reference into the Consolidated Amended Complaint, which relies on it heavily. See, e.g., Compl., ¶¶ 30-62, 114-17.

affected parties free credit monitoring and identity-theft protection and restoration services for one year. See id.

Still, Plaintiffs claim that the data breach caused them substantial harm. Twenty-four of the thirty-three Plaintiffs here allege that they have been injured because of the disclosure alone.[3] They claim that, even if no one has yet used their personal information, they face an increased risk of identity theft, which they view as a distinct and palpable harm. See Compl., ¶¶ 20, 23. They also claim that the data breach violated their expectation of privacy, as codified in various statutes, state tort law, and possibly through contract. See id., ¶¶ 1, 20, 21, 24. In addition, five of those twenty-four Plaintiffs claim that they have spent time or money monitoring their credit or interfacing with their banks since the theft, and that their time and effort should be compensable.[4]

Six Plaintiffs also claim that someone used their credit cards or bank accounts without their authorization, although no one alleges that financial information was actually on the stolen tapes.[5] One of those six additionally claims that loans have been opened in his name using his personal information – presumably including his social security number, name, date of birth, and address, all of which were on the backup tapes.[6] Yet another Plaintiff alleges that she was harmed because her medical identity has disappeared.[7] Finally, two Plaintiffs allege that they have received unwanted phone calls or "phishing" emails, and one of those Plaintiffs claims that marketers have information about her medical condition that they likely obtained from the tapes.[8]

---

[3] Compl., ¶¶ 30 (Adcock), 31 (Arellano), 32 (Bacon), 33 (Bates), 34 (Biggerman), 36 (Deatrick), 37 (Erickson), 39 (Hartman), 42 (Johnson), 44 (Losack), 45 (Martin), 46 (Moss-McUmber), 47 (Miller), 50 (Newman), 51 (O'Hara-Epperly), 52 (Palmer), 53 (Peting), 54 (Pineirovigo), 55 (Reznikov), 56 (Richardson), 57 (Roe), 58 (Trower), 59 (Walters), 61 (Worrell).

[4] Compl., ¶¶ 37 (Erickson), 44 (Losack), 52 (Palmer), 56 (Richardson), 59 (Walters).

[5] Compl., ¶¶ 35 (Curtis), 38 (Gaffney), 40 (Hawk), 41 (Hernandez), 43 (Keller), 48 (Morelli).

[6] Compl., ¶ 35 (Curtis).

[7] Compl., ¶ 60 (Warner).

[8] Compl., ¶¶ 49 (Moskowitz), 62 (Yarde).

Plaintiffs filed this lawsuit against TRICARE, which is a government agency that provides insurance coverage and health care to active-duty service members and their families, see 10 U.S.C. §§ 1074, 1076, 1079; 32 C.F.R. pt. 199; Compl., ¶ 3, [9] and against the Department of Defense and its Secretary. The breach victims are also suing SAIC, a security firm that contracts with TRICARE to ensure the security of the personally identifiable information (PII) and protected health information (PHI) in its records. See Compl., ¶ 67.

In their Consolidated Amended Complaint, Plaintiffs allege no fewer than twenty separate causes of action, ranging from the violation of various federal statutes – such as the Privacy Act, the Fair Credit Reporting Act, and the Administrative Procedure Act – to the contravention of state statutes and common law – such as claims of negligence, breach of contract, and violation of various state consumer-protection laws. The injuries alleged include: (i) increased risk of identity theft, which Plaintiffs peg at 9.5 times their pre-theft risk; (ii) expenses incurred in mitigating the risk of identity theft; (iii) loss of privacy through the exposure of their personal information; (iv) loss of the value of their personal and medical information; (v) loss of the value of their insurance premiums, which should have been used to pay for proper security measures; (vi) SAIC's failure to meet the requisite standard for data security; (vii) the lost right to truthful information about their data security; (viii) statutory (or liquidated) damages; and, in at least one case, (ix) actual identity theft. Compl., ¶¶ 20-23. The Court will address each theory of injury in turn as it analyzes the standing of Plaintiffs to proceed.

[9] At the time this suit was filed, TRICARE was overseen by a group called Tricare Management Activity, which is the entity Plaintiffs originally sued. TMA has since been disestablished, and the Defense Health Agency has taken over TMA's duties. See TMA, Defense Health Agency, http://www.tricare.mil/tma/ (last visited May 1, 2014). For ease, the Court refers to both TRICARE and its management agency jointly as TRICARE.

B. Procedural Background

This action encompasses eight separate cases filed in four different courts around the country. While most of those actions originated here in D.C., others were transferred from the Northern and Southern Districts of California as well as the Western District of Texas. See ECF No. 1 (Transfer Order) at 1-3. Consolidation of those cases for pretrial purposes took effect in June 2012, id., and in August of that year the Court held a hearing to sort out the administrative details of the newly combined multi-district litigation. See ECF No. 13 (Hearing Tr.) at 6. In October 2012, Plaintiffs filed a Consolidated Amended Complaint encompassing the allegations of thirty-three Plaintiffs from twenty-four states. See Compl., ¶¶ 1, 154. In November 2012, Defendants moved to dismiss all thirty-three Plaintiffs for lack of standing or, in the alternative, to dismiss each cause of action as unsupported by the factual allegations in the Complaint. Since that time, Plaintiffs have moved to supplement their pleadings, Defendants have filed multiple notices of supplemental authority, and the case has been reassigned from one judge to another.

Having recently taken the reins, this Court now addresses the first major issue raised by the Motions to Dismiss: standing.

II. Legal Standard

Because this Opinion addresses only Defendants' jurisdictional arguments, Federal Rule of Civil Procedure 12(b)(1) provides the relevant legal standard.

In evaluating Defendants' Motions to Dismiss, then, the Court must "treat the complaint's factual allegations as true . . . and must grant plaintiff 'the benefit of all inferences that can be derived from the facts alleged.'" Sparrow v. United Air Lines, Inc., 216 F.3d 1111, 1113 (D.C. Cir. 2000) (quoting Schuler v. United States, 617 F.2d 605, 608 (D.C. Cir. 1979)) (internal citation omitted); see also Jerome Stevens Pharms., Inc. v. FDA, 402 F.3d 1249, 1253

(D.C. Cir. 2005). This standard governs the Court's considerations of Defendants' Motions under both Rules 12(b)(1) and 12(b)(6). See Scheuer v. Rhodes, 416 U.S. 232, 236 (1974) ("in passing on a motion to dismiss, whether on the ground of lack of jurisdiction over the subject matter or for failure to state a cause of action, the allegations of the complaint should be construed favorably to the pleader"); Walker v. Jones, 733 F.2d 923, 925-26 (D.C. Cir. 1984) (same). The Court need not accept as true, however, "a legal conclusion couched as a factual allegation," nor an inference unsupported by the facts set forth in the Complaint. Trudeau v. Fed. Trade Comm'n, 456 F.3d 178, 193 (D.C. Cir. 2006) (quoting Papasan v. Allain, 478 U.S. 265, 286 (1986)) (internal quotation marks omitted). In addition, the "complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009) (quoting Bell Atlantic Corp. v. Twombly, 550 U.S. 54, 570 (2007)).

To survive a motion to dismiss under Rule 12(b)(1), Plaintiffs bear the burden of proving that the Court has jurisdiction to hear their claims. See Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992); U.S. Ecology, Inc. v. U.S. Dep't of Interior, 231 F.3d 20, 24 (D.C. Cir. 2000). A court has an "affirmative obligation to ensure that it is acting within the scope of its jurisdictional authority." Grand Lodge of Fraternal Order of Police v. Ashcroft, 185 F. Supp. 2d 9, 13 (D.D.C. 2001). For this reason, "'the [p]laintiff's factual allegations in the complaint . . . will bear closer scrutiny in resolving a 12(b)(1) motion' than in resolving a 12(b)(6) motion for failure to state a claim." Id. at 13-14 (quoting 5A Charles A. Wright & Arthur R. Miller, Federal Practice and Procedure § 1350 (2d ed. 1987)) (alteration in original). Additionally, unlike with a motion to dismiss under Rule 12(b)(6), the Court "may consider materials outside the pleadings in deciding whether to grant a motion to dismiss for lack of jurisdiction." Jerome Stevens

Pharms., 402 F.3d at 1253; see also Venetian Casino Resort, LLC v. EEOC, 409 F.3d 359, 366 (D.C. Cir. 2005); Herbert v. Nat'l Academy of Sciences, 974 F.2d 192, 197 (D.C. Cir. 1992).

III. Analysis

Before examining the merits of any claim, courts must begin with questions of jurisdiction. See Fla. Audubon Soc'y v. Bentsen, 94 F.3d 658, 663 (D.C. Cir. 1996) (*en banc*). Plaintiffs' first battle, then, is to prove that they have standing to pursue their claims. See Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 93-95 (1998). That, as it turns out, is an uphill climb for all but two of the named Plaintiffs.

Article III of the Constitution limits the power of the federal judiciary to the resolution of "Cases" and "Controversies." U.S. Const. art. III, § 2; see also Allen v. Wright, 468 U.S. 737, 750 (1984) (discussing the case-or-controversy requirement). Because "standing is an essential and unchanging part of the case-or-controversy requirement of Article III," Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992), standing is a necessary "predicate to any exercise of [the Court's] jurisdiction." Fla. Audubon Soc'y, 94 F.3d at 663.

"Every plaintiff in federal court," consequently, "bears the burden of establishing the three elements that make up the 'irreducible constitutional minimum' of Article III standing: injury-in-fact, causation, and redressability." Dominguez v. UAL Corp., 666 F.3d 1359, 1362 (D.C. Cir. 2012) (quoting Lujan, 504 U.S. at 560-61). Even in the class-action context, all named Plaintiffs "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." Warth v. Seldin, 422 U.S. 490, 502 (1975) (emphasis added). Each element of standing must be pled or proven with the requisite "degree of evidence required at the successive stages of the litigation." Lujan, 504 U.S. at 561. That is, at the motion-to-dismiss

stage, Plaintiffs must plead facts that, taken as true, make the existence of standing plausible. See Galaria v. Nationwide Mut. Ins. Co., Nos. 13-118, 13-257, 2014 WL 689703, at *3 (S.D. Ohio Feb. 10, 2014) (emphasis added). In "considering whether a plaintiff has Article III standing, a federal court must assume *arguendo* the merits of his or her legal claim." Parker v. District of Columbia, 478 F.3d 370, 377 (D.C. Cir. 2007), aff'd on other grounds sub nom. District of Columbia v. Heller, 554 U.S. 570 (2008).

A. Injury in Fact

The Court will examine each element of standing in turn, beginning with injury in fact. An injury in fact is "an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical." Lujan, 504 U.S. at 560 (citations and internal quotation marks omitted). "Allegations of possible future injury do not satisfy the requirements of Art. III. A threatened injury must be certainly impending to constitute injury in fact." Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (internal quotation marks omitted) (emphasis added).

The Supreme Court recently reviewed the contours of this requirement in Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013). There, plaintiffs – who were attorneys and human-rights, labor, legal, and media organizations who worked with foreign clients or sources – contended that they were likely to be targeted for surveillance under the Foreign Intelligence Surveillance Act. See id. at 1145-46. This, they claimed, would work them harm. As such, they had taken steps to keep conversations with their clients confidential at their own personal expense. See id. The Court held, however, that plaintiffs did not have an injury in fact because the threat of surveillance was too speculative. There were, the Court reasoned, simply too many "ifs" involved before an injury came to pass. The plaintiffs would be impacted by FISA only if

(1) the government decided to target communications involving their clients and (2) used the challenged FISA provision to do so, (3) the Foreign Intelligence Surveillance Court authorized the eavesdropping, (4) the government succeeded in picking up their targets' phone calls or e-mails, and, finally, (5) the plaintiffs were involved in whatever communication the government intercepted. Id. at 1147-48. The Court concluded that such "a highly attenuated chain of possibilities[] does not satisfy the requirement that threatened injury must be certainly impending." Id. at 1148; see also Whitmore, 495 U.S. at 156-57 (speculative to assume that petitioner would request federal habeas review; habeas would be granted; petitioner would be retried for his capital offense; and thus, on appeal from this new trial, petitioner would suffer due to a lack of data on similarly situated criminal defendants); O'Shea v. Littleton, 414 U.S. 488, 496-97 (1974) (injury speculative where plaintiff would need to violate the law, be arrested, and be tried before a specific magistrate judge to be harmed by the judge's allegedly illegal courtroom practice); Los Angeles v. Lyons, 461 U.S. 95, 105-09 (1983) (injury conjectural or hypothetical where plaintiff would have to commit an illegal act, be arrested, and be subjected to a chokehold in the future for injury to occur).

The Court added, "Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm" was also "unavailing – because the harm respondents seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." Clapper, 133 S. Ct. at 1151.

With those precepts in mind – that an injury must be present or certainly impending, that an attenuated chain of possibilities does not confer standing, and that plaintiffs cannot create

standing by taking steps to avoid an otherwise speculative harm – the Court turns to Plaintiffs' allegations of injury here.

1. Increased Risk of Harm and Monitoring Costs

Plaintiffs begin by asserting that an increased risk of harm alone constitutes an injury sufficient to confer standing to sue. Due to the data breach, they claim that they are 9.5 times more likely than the average person to become victims of identity theft. Compl., ¶ 23. That increased risk, they maintain, in and of itself confers standing. But as Clapper makes clear, that is not true. The degree by which the risk of harm has increased is irrelevant – instead, the question is whether the harm is certainly impending. See also Public Citizen, Inc. v. Nat'l Highway Traffic Safety Admin., 489 F.3d 1279, 1297-98 (D.C. Cir. 2007) ("'increased risk' is" not by "itself [a] concrete, particularized, and actual injury for standing purposes" – harm must be "actual" or "imminent," not merely "increased").

Here, the relevant harm alleged is identity theft. A handful of Plaintiffs claims that they have suffered actual identity theft, and those Plaintiffs have clearly suffered an injury. At least twenty-four, however, allege only a risk of identity theft. See *supra* n.3. At this point, the likelihood that any individual Plaintiff will suffer harm remains entirely speculative. For identity theft to occur, after all, the following chain of events would have to transpire: First, the thief would have to recognize the tapes for what they were, instead of merely a minor addition to the GPS and stereo haul. Data tapes, after all, are not something an average computer user often encounters. The reader, for example, may not even be aware that some companies still use tapes – as opposed to hard drives, servers, or even CDs – to back up their data. See Disk or Tape Backup: Which is Best?, Backup For Servers, http://goo.gl/7JsXQF (last visited Apr. 28, 2014). Then, the criminal would have to find a tape reader and attach it to her computer. Next, she

would need to acquire software to upload the data from the tapes onto a computer – otherwise, tapes have to be slowly spooled through like cassettes for data to be read. Id. After that, portions of the data that are encrypted would have to be deciphered. See Compl., ¶ 95 ("a portion of the PII/PHI on the data tapes was encrypted"). Once the data was fully unencrypted, the crook would need to acquire a familiarity with TRICARE's database format, which might require another round of special software. Finally, the larcenist would have to either misuse a particular Plaintiff's name and social security number (out of 4.7 million TRICARE customers) or sell that Plaintiff's data to a willing buyer who would then abuse it.

The vast majority of Plaintiffs has not alleged that any of those things have happened – because they cannot. Those events are entirely dependent on the actions of an unknown third party – namely, the thief. At this point, we do not know who she was, how much she knows about computers, or what she has done with the tapes. The tapes could be uploaded onto her computer and fully deciphered, or they could be lying in a landfill somewhere in Texas because she trashed them after achieving her main goal of boosting the car stereo and GPS. Unfortunately, there is simply no way to know until either the crook is apprehended or the data is actually used. Courts for this reason are reluctant to grant standing where the alleged future injury depends on the actions of an independent third party. See Clapper, 133 S. Ct. at 1150 (expressing "our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors").

That is, no doubt, cold comfort to the millions of servicemen and women who must wait and watch their credit reports until something untoward occurs. After all, it is reasonable to fear the worst in the wake of such a theft, and it is understandably frustrating to know that the safety of your most personal information could be in danger. The Supreme Court, however, has held

that an "objectively reasonable likelihood" of harm is not enough to create standing, even if it is enough to engender some anxiety. See id., 133 S. Ct. at 1147-48. Plaintiffs thus do not have standing based on risk alone, even if their fears are rational.

Nor is the cost involved in preventing future harm enough to confer standing, even when such efforts are sensible. See id. at 1150-51. There is, after all, nothing unreasonable about monitoring your credit after a data breach. In fact, that is exactly what TRICARE and SAIC advised Plaintiffs to do – and what SAIC, in part, offered to pay for. See, e.g., Letter from SAIC at 1. But the Supreme Court has determined that proactive measures based on "fears of . . . future harm that is not certainly impending" do not create an injury in fact, even where such fears are not unfounded. Clapper, 133 S. Ct. at 1151. Put another way, the Court has held that plaintiffs cannot create standing by "inflicting harm on themselves" to ward off an otherwise speculative injury. Id. The cost of credit monitoring and other preventive measures, therefore, cannot create standing.

There is, however, an alternative argument. Plaintiffs point out that, in Clapper, the Court acknowledged that it sometimes "found standing based on a 'substantial risk' that . . . harm will occur, which [could] prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." Clapper, 133 S. Ct. at 1150 n.5 (emphasis added). So Plaintiffs could, theoretically, prevail if the risk of harm here were substantial. Yet, Plaintiffs' Complaint itself makes clear that they do not surmount that hurdle. To be sure, Plaintiffs allege that data-breach victims in general are 9.5 times more likely than the average person to experience identity theft post-breach. Compl., ¶ 132. But then Plaintiffs note that, overall, only about 19% of breach victims actually experience identity theft. Id. By Plaintiff's own calculations, then, injury is likely not impending for over 80% of victims – and the figure is likely to be considerably higher in this

case, where the theft was unsophisticated and where the lack of widespread harm suggests that the tapes have not ever been accessed. Cf. Galaria, 2014 WL 689703, at *5. The harm in these circumstances, therefore, cannot satisfy the requirement of either the Supreme Court or the D.C. Circuit that there be "(i) a substantially increased risk of harm and (ii) a substantial probability of harm with that increase taken into account." Public Citizen, Inc., 489 F.3d at 1295.

The conclusion that an increased risk of harm alone does not confer standing is supported by other courts' analyses in similar data-breach cases. In Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011), for example, a payroll company's database was hacked, possibly exposing "employees' names, addresses, social security numbers, dates of birth, and bank account information." Id. at 40. Still, the Third Circuit held that, where it was "not known whether the hacker read, copied, or understood the data," injury remained speculative. Id. In Randolph v. ING Life Insurance & Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007), an unknown crook pilfered a laptop containing insurance information, including the "names, addresses, and Social Security numbers" of customers. Id. at 3. Nonetheless, because plaintiffs did "not allege that the burglar who stole the laptop did so in order to access their Information, or that their Information has actually been accessed since the laptop was stolen," it was "mere speculation" to assume "that at some unspecified point in the indefinite future they w[ould] be the victims of identity theft." Id. at 7-8; see also Whitaker v. HealthNet of Cal., Inc., No. 11-910, 2012 WL 174961, at *2 (E.D. Cal. Jan. 20, 2012) ("[P]laintiffs do not explain how the loss here has actually harmed them . . . or that third parties have accessed their data. Any harm stemming from their loss thus is precisely the type of conjectural and hypothetical harm that is insufficient to allege standing.") (footnote omitted); Hammond v. Bank of N.Y. Mellon Corp., No. 08-6060, 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010) ("Plaintiffs lack standing" where backup data tapes were stolen

and most plaintiffs alleged only a risk of harm "because their claims are future-oriented, hypothetical, and conjectural."); Allison v. Aetna, Inc., No. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010) ("Plaintiff's alleged injury of an increased risk of identity theft is far too speculative."); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1052 (E.D. Mo. 2009) (no standing where "plaintiff does not claim that his personal information has in fact been stolen and/or his identity compromised" in the data breach); Bell v. Acxiom Corp., No. 06-485, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) ("[W]hile there have been several lawsuits alleging an increased risk of identity theft, no court has considered the risk itself to be damage. Only where the plaintiff has actually suffered identity theft has the court found that there were damages.") (footnote omitted); Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006) (In data-breach case, "plaintiff's allegations, if true, create only the possibility of harm at a future date. Plaintiff[] alleges that her potential injury is contingent upon her information being obtained and then used by an unauthorized person for an unlawful purpose.") (citation omitted); Giordano v. Wachovia Sec., LLC, No. 06-476, 2006 WL 2177036, at *5 (D.N.J. July 31, 2006) ("Plaintiff only alleges a potential injury (identity theft) that is contingent on (1) Plaintiff's information falling into the hands of an unauthorized person and (2) that person using such information for unlawful purposes to Plaintiff's detriment.").

Litigants' cost-of-monitoring claims fared no better. See, e.g., Reilly, 664 F.3d at 46 ("Appellants' alleged time and money expenditures to monitor their financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for Appellants' claims."); Randolph, 486 F. Supp. 2d at 8 (The "argument that the time and money spent monitoring a plaintiff's credit suffices to establish an

injury overlook[s] the fact that their expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized.") (internal quotation marks omitted).

This is not to say that courts have uniformly denied standing in data-breach cases. See, e.g., Holmes v. Countrywide Fin. Corp., No. 08-205, 2012 WL 2873892, at *5-*11(W.D. Ky. July 12, 2012); McLoughlin v. People's United Bank, Inc., No. 08-944, 2009 WL 2843269, at *3-*4 (D. Conn. Aug. 31, 2009); Doe 1 v. AOL, 719 F. Supp. 2d 1102, 1109 (N.D. Cal. 2010); Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 279-80 (S.D.N.Y. 2008). Most cases that found standing in similar circumstances, however, were decided pre-Clapper or rely on pre-Clapper precedent and are, at best, thinly reasoned. For example, in Ruiz v. Gap, Inc., 380 Fed. Appx. 689 (9th Cir. 2010) (Gap III), the court stated that a "credible threat of harm is sufficient to constitute actual injury for standing purposes." Id. at 691; see also, e.g., Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) ("the possibility of future injury may be sufficient to confer standing on plaintiffs; threatened injury constitutes 'injury in fact'") (quoting Cent. Delta Water Agency v. United States, 306 F.3d 938, 947 (9th Cir. 2002)); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (standing because "the scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious"). Yet after Clapper, Gap III's "credible threat of harm" standard is clearly not supportable.

Indeed, since Clapper was handed down last year, courts have been even more emphatic in rejecting "increased risk" as a theory of standing in data-breach cases. As one court noted, after "Clapper, the mere fact that the risk has been increased does not suffice to establish standing." Strautins v. Trustwave Holdings, Inc., No. 12-9115, 2014 WL 960816, at *4 (N.D. Ill. Mar. 12, 2014). After all, an increased risk or credible threat of impending harm is plainly

different from certainly impending harm, and certainly impending harm is what the Constitution and Clapper require. Clapper, 133 S. Ct. at 1148; see, e.g., Strautins, 2014 WL 960816, at *4 (deciding in light of Clapper that injury was speculative based "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"); Galaria, 2014 WL 689703, at *5 (noting the similarity to Clapper and holding that "[i]n this case, an increased risk of identity theft, identity fraud, medical fraud or phishing is not itself an injury-in-fact because Named Plaintiffs did not allege – or offer facts to make plausible – an allegation that such harm is 'certainly impending'"); Polanco v. Omnicell, Inc., No. 13-1417, 2013 WL 6823265, at *14 (D.N.J. Dec. 26, 2013) (relying on Clapper and Reilly to conclude that mere loss of data, without misuse, is not "an injury sufficient to confer standing"); but see In re Sony Gaming Networks & Customer Data Sec. Breach Litigation, MDL No. 11-2258, 2014 WL 223677, at *9 (S.D. Cal. Jan. 21, 2014) (finding standing post-Clapper based on a "plausibly alleged . . . 'credible threat' of impending harm").

In sum, increased risk of harm alone does not constitute an injury in fact. Nor do measures taken to prevent a future, speculative harm. At least twenty-four of the thirty-three Plaintiffs in this case, then, must rely on an alternative theory of injury.

2. Privacy

Plaintiffs also allege that they have been injured because their privacy was invaded by the data breach. Yet this claim suffers from the same defects as Plaintiffs' previous contention. For a person's privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party. Existing case law and legislation support that common-sense intuition: If no one has viewed your private information (or is about to view it imminently), then your privacy has

not been violated. See, e.g., 5 C.F.R. § 297.102 (Under Privacy Act, "[d]isclosure means providing personal review of a record, or a copy thereof, to someone other than the data subject or the data subject's authorized representative, parent, or legal guardian.") (emphasis added); Walia v. Chertoff, No. 06-6587, 2008 WL 5246014, at *11 (E.D.N.Y. Dec. 17, 2008) ("accessibility" is not the same as "active disclosure"); Schmidt v. Dep't of Veterans Affairs, 218 F.R.D. 619, 630 (E.D. Wisc. 2003) (Disclosure is "the placing into the view of another information which was previously unknown," requiring that information be "actually viewed."); Harper v. United States, 423 F. Supp. 192, 197 (D.S.C. 1976) (Disclose means "the imparting of information which in itself has meaning and which was previously unknown to the person to whom it was imparted."); Fairfax Hosp. v. Curtis, 492 S.E. 2d 642, 644 (Va. 1997) (violation where third party "possess[ed]" and "reviewed" records).

Here, the majority of Plaintiffs contend neither that their personal information has been viewed nor that their information has been exposed in a way that would facilitate easy, imminent access. As in the Third Circuit case Reilly, it would be speculative to assume that the thief "read, copied, or understood the data." 664 F.3d at 40. As a result, no invasion of Plaintiffs' privacy is imminent. See also Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012) (dismissing privacy claim for lack of standing where information had not been viewed by third party); Allison, 2010 WL 3719243 (no standing in data-breach case, even where claim involved invasion of privacy); Giordano, 2006 WL 2177036 (same); Strautins, 2014 WL 960816 (same); but see Galaria, 2014 WL 689703 (allowing standing for certain claims based only on invasion of privacy); Am. Fed'n of Gov't Emps. v. Hawley, 543 F. Supp. 2d 44, 50 n.12 (D.D.C. 2008) ("emotional trauma alone is sufficient to qualify as an" injury "under Section 552a(g)(1)(D) of the Privacy Act") (internal quotation marks and alterations omitted).

To be sure, the Supreme Court has intimated that disclosure of personally identifiable information alone, along with some attendant emotional distress, may constitute "injury enough to open the courthouse door" in privacy actions. Doe v. Chao, 540 U.S. 614, 624-25 (2004). But again, disclosure involves publication to a third party. In that case, Doe's social security number had actually been published by the government on various documents "sent to groups of [workers'-compensation] claimants, their employers, and the lawyers involved in their cases." Id. at 617. In other words, Doe's information was actually exposed to dozens of readers. Here, by contrast, disclosure and access of Plaintiffs' personal information is anything but certain. Rather, the information itself is locked inside tapes that require some expertise to open and decipher. Indeed, it is highly unlikely that the crook even understood what the tapes were, let alone had the wherewithal to access them or navigate her way to any one of the 4.7 million records contained therein. And until Plaintiffs can aver that their records have been viewed (or certainly will be viewed), any harm to their privacy remains speculative.

A few of the Plaintiffs here do allege that their data was used.[10] Those Plaintiffs have at least claimed an injury to their privacy insofar as they allege that their data was accessed. The other Plaintiffs, however, are out of luck.

3. Loss of Value

Plaintiffs next contend that they were injured by the loss of two valuable assets. First, they argue that they lost the value of their personal and medical information, which could be "sold on the cyber black market for $14 to $25 per medical record." Compl., ¶ 21. Second, they claim they forfeited the value of their insurance premiums, which should have been used to pay for better security. See id., ¶ 22.

[10] Compl., ¶¶ 35 (Curtis), 38 (Gaffney), 40 (Hawk), 41 (Hernandez), 43 (Keller), 48 (Morelli), 49 (Moskowitz), 62 (Yarde).

As to the value of their personal and medical information, Plaintiffs do not contend that they intended to sell this information on the cyber black market in the first place, so it is uncertain how they were injured by this alleged loss. Even if the service members did intend to sell their own data – something no one alleges – it is unclear whether or how the data has been devalued by the breach. For those reasons, Plaintiffs' first theory of injury is unsuccessful.

Similarly, as to the value of their insurance premiums, Plaintiffs do not plausibly allege any actual loss. They allege that they were paying for "health and dental insurance" – and they do not claim that they were denied coverage or services in any way whatsoever. See id. To the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing. They do not maintain, moreover, that the money they paid could have or would have bought a better policy with a more bullet-proof information-security regime. Put another way, Plaintiffs have not alleged facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid. Nothing in the Complaint makes a plausible case that Plaintiffs were cheated out of their premiums. As a result, no injury lies.

4. Legal Violations

Plaintiffs next set forth various legal violations that they claim create standing: They argue that SAIC failed to meet the requisite legal standards for data security; that SAIC and TRICARE violated their right to truthful information about their data; and that certain statutes, if violated, give them the right to automatic damages or payment. Standing, however, does not merely require a showing that the law has been violated, or that a statute will reward litigants in general upon showing of a violation. Rather, standing demands some form of injury – some

showing that the legal violation harmed you in particular, and that you are therefore an appropriate advocate in federal court.

As the Supreme Court "has repeatedly held . . .[,] an asserted right to have the [defendant] act in accordance with law is not sufficient, standing alone, to confer jurisdiction on a federal court." Allen v. Wright, 468 U.S. 737, 754 (1984). Rather, the unlawful activity must work some harm on Plaintiffs.

In terms of the alleged contravention of security standards, Plaintiffs have not outlined any actual or imminent harm caused by that purported violation – aside from the theories the Court has already rejected. Plaintiffs, therefore, cannot acquire standing on that basis.

The same is true of the supposed deprivation of Plaintiff's "right to truthful information about the security of their PII/PHI." Opp. to SAIC at 7. No independent harm has flowed from that so-called deprivation. Of course, as Plaintiffs point out, denial of information alone can sometimes create an injury when statutes require disclosure. See Zivotofsky ex rel. Ari Z. v. Sec'y of State, 444 F.3d 614, 617-19 (D.C. Cir. 2006) (noting that violation of plaintiff's right to documents under Freedom of Information Act can create standing). Here, however, Plaintiffs have failed to allege any actual deprivation of information, even assuming they have a right to it. First, they claim that they were deprived of information before TRICARE and SAIC notified them of the data breach. Any injury that might have occurred during that time, however, has been cured, since SAIC has now explained the extent of the breach to Plaintiffs in some detail, see Letter from SAIC at 1, and no one alleges any independent harm caused by the delay. Indeed, expedient notification of the data breach and its scope, along with certain required contact information, is all the relevant laws demand. See, e.g., Cal. Civ. Code § 1798.82; Or. Rev. Stat. Ann. § 646A.604(1)-(2). In addition, Plaintiffs claim that they have been deprived of

truthful information because SAIC "[c]ategoriz[ed] the risk of access" to their data "as 'low'" in their letters notifying servicemen of the breach. Compl., ¶ 116. But that is, at best, a difference of opinion – Plaintiffs do not identify any actual facts that SAIC or TRICARE has withheld. As a result, Plaintiffs' abstract assertion that their "right to truthful information" has been violated does not constitute an injury, since the facts in the complaint identify neither an actual deprivation nor any independent harm.

5. Actual Misuse

As noted above, Plaintiffs who claim that their information was, in fact, accessed and misused have alleged an actual injury. That injury, however, must still be linked to Defendants' conduct.

B. Causation

The second element of standing, causation, requires "a causal connection between the injury and the conduct complained of." Lujan, 504 U.S. at 560. The harm alleged must be "fairly . . . trace[able] to the challenged action of the defendant, and not injury that results from the independent action of some third party not before the court." Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41-42 (1976).

To review the bidding: The majority of Plaintiffs in this case lack standing to sue because they failed to allege any cognizable injury. Six Plaintiffs, however, claim that their data was actually misused; one Plaintiff claims she has suffered medical fraud; and two claim that their privacy was invaded by phone calls and other solicitations from companies that may have accessed their medical records. Each of these three groups of Plaintiffs must be able to link their harm to the data breach.

1. Identity Theft

Six out of thirty-three Plaintiffs allege that their personal information was used for fraudulent purposes. See *supra* n.5. Five of those six claim only that unauthorized charges were made to their existing credit cards or debit cards, or that money was withdrawn from an existing bank account. But here's the problem: No one alleges that credit-card, debit-card, or bank-account information was on the stolen tapes. See, e.g., Letter from SAIC at 1 (tapes did not include "any financial data, such as credit card or bank account information"). To be sure, as Plaintiffs' counsel noted at the Court's August hearing, a criminal could obtain some of a victim's personal information from a data breach and then go "phishing" to get the rest. See Hrg. Tr. at 45-46. That is, the crook could acquire a name and phone number and then make calls pretending to be a legitimate business asking for information like credit-card or bank-account numbers. Here, however, the identity-theft Plaintiffs have not alleged any phishing. Indeed, they proffer no plausible explanation for how the thief would have acquired their banking information. In a society where around 3.3% of the population will experience some form of identity theft – regardless of the source – it is not surprising that at least five people out of a group of 4.7 million happen to have experienced some form of credit or bank-account fraud. See Kristin Finklea, Cong. Research Serv., R40599, Identity Theft: Trends and Issues 1 (2014), available at http://goo.gl/bCsTEg (10.2 million Americans, out of around 308.7 million total, experienced identity theft in 2010). As that information was not on the tapes, though, Plaintiffs cannot causally link it to the SAIC breach.

One Plaintiff, however – Robert Curtis, a Colorado resident – may have a case.[11] After the data breach, he received "letters in the mail from American Express," among others,

[11] Plaintiffs have moved to supplement their factual allegations concerning Curtis. See ECF No. 41 (Motion for Leave to File Supplemental Pleadings). The Court grants that Motion here, although it notes that its

"thanking him for applying for loans" that he had never applied for. Compl., ¶ 35. To apply for such a loan, one would likely need a person's name, address, date of birth, and social security number – exactly the sort of information that was on the tapes. Id., ¶ 7. The Court believes that this creates a sufficient causal link between the identity theft – which has hurt Curtis's credit history, id., ¶ 35 – and the tape theft.

That said, the Court would be remiss if it did not note that Curtis also alleges a spate of identity theft that cannot plausibly be linked to the tapes. For example, he also complains that many of his existing accounts have been tampered with in seriously concerning and, no doubt, frustrating ways. Id. In one instance, Curtis's bank notified him when "an individual in Mexico" called his bank asking for money "and knew Plaintiff Curtis' account number, unlisted telephone number, address, date of birth and e-mail address, Social Security number and answers to the security questions." ECF No. 43 (Reply to Motion to Supplement Pleadings), Exh. A (Supplement to Compl., ¶ 35) at 1. No one alleges, however, that the name of Curtis's bank, his account number, his e-mail address, or the answers to his security questions were on the stolen tapes. He also claims that "individuals wired approximately $32,500 out of his credit union account." Id. But again, he does not claim that the account information was on the tapes, although he does aver that he gave TRICARE his payment information at some point. Id. The inescapable conclusion is that Curtis has been subjected to another, more profound data breach involving his financial – not medical – records.

As a result, the fraudulent loan applications may also be linked to this other, more severe data breach and not the SAIC breach. At this point, however, the Court is willing to give Curtis

---

conclusions regarding Curtis would be the same under both the original and the amended pleadings.

the benefit of the doubt, since there is at least a plausible connection between some of the harm he has suffered and the SAIC theft.

2. Medical Fraud

Another Plaintiff, Robin Warner, claims that she experienced medical fraud because her medical records no longer exist. Compl., ¶ 60. This is a striking allegation, but it cannot establish standing because only backup tapes were stolen from the SAIC employee's car. Id., ¶ 6. Warner does not explain how the disappearance of her medical identity can be linked to the theft of tapes that contained only copies of her actual medical records. She has thus not carried her burden of alleging causation and hence has no standing.

3. Privacy

Two final Plaintiffs – in addition to Curtis, who has experienced similar woes – claim that their privacy has been invaded due to the data breach. Murray Moskowitz simply alleges that he "has received a number of unsolicited calls from telemarketers and scam artists." Id., ¶ 49. He does not otherwise link the calls to the tapes, claim that the callers have personal or private information found on the tapes, or even allege that his phone number was unlisted and hence would have been difficult for marketers to locate absent the assistance of the data thief. Moskowitz seems to simply be one among the many of us who are interrupted in our daily lives by unsolicited calls. His harm, consequently, cannot plausibly be linked to the tapes.

Dorothy Yarde, on the other hand, does allege a credible link to the data breach. She claims that her "telephone number is unlisted." Id., ¶ 62. Still, after the theft, "she received numerous unsolicited telephone calls from insurance companies and other[s]" pitching "medical products and services . . . targeted at a specific medical condition listed in her medical records." Id. (emphasis added). She had not received such calls in the past. Id. The fact that the callers

had Yarde's unlisted phone number and medical diagnosis – both of which were on the tapes – suffices to create a causal link.

C. Redressability

The third and final element of standing is redressability, which requires that it "be 'likely,' as opposed to merely 'speculative,' that the" alleged "injury will be 'redressed by a favorable decision.'" Lujan, 504 U.S. at 561 (citation omitted).

At this point, only two Plaintiffs remain: Curtis, who has alleged actual misuse of his social security number, and Yarde, who has alleged a privacy violation linked to her medical information. Both harms can be redressed, at least in part, by a monetary reward. Those two Plaintiffs – and only those two Plaintiffs – therefore have standing to sue.

* * *

A reasonable reader may still wonder: If Curtis and Yarde's information was potentially accessed or misused, why not presume that the remaining Plaintiffs' information will suffer the same fate? Indeed, other courts have allowed cases to move forward where some form of fraud had already taken place. For example, in Anderson v. Hannaford Bros., 659 F.3d 151 (1st Cir. 2011), the First Circuit declined to question the plaintiffs' standing where 1,800 instances of credit- and debit-card fraud had already occurred and had been clearly linked to the data breach. Id. at 162-67. Similarly, in Pisciotta, the court allowed plaintiffs to proceed where "the scope and manner of access suggest[ed] that the intrusion was sophisticated, intentional and malicious," and thus that the potential for harm was indeed substantial. 499 F.3d at 632.

The circumstances here, however, are starkly different. First, the theft from the SAIC employee's car was a low-tech, garden-variety one. Any inference to the contrary is undermined by the snatching of the GPS and car stereo. This is hardly a black-ops caper. Second, while

Curtis and Yarde have alleged personalized injury sufficient to surmount a motion to dismiss under Rule 12(b)(1), there are no facts here that plausibly point to imminent, widespread harm. In fact, the link between Curtis and Yarde's injuries and the data breach barely crosses the line from possible to plausible. Curtis, after all, was almost certainly the victim of another, more severe data breach, and that breach may well have been responsible for every instance of identity theft he alleges. It remains likely, in other words, that no one accessed his information from the tapes. Yarde's harm may also stem from another source. For example, she might have bought specific medications related to her condition over the counter at the neighborhood drugstore or online. That information could have been sold to companies targeting such patients – no data breach necessary. At this stage, the Court simply acknowledges that the link between the data breach and Yarde and Curtis's claims is plausible, even if it is very likely that their harm stems from another source.

The fact that Curtis and Yarde's allegations are plausible, however, does not lead to the conclusion that wide-scale disclosure and misuse of all 4.7 million TRICARE customers' data is plausibly "certainly impending." Clapper, 133 S. Ct. at 1147. After all, as previously noted, roughly 3.3% of Americans will experience identity theft of some form, regardless of the source. See Finklea, Identity Theft: Trends and Issues, *supra*, at 1. So one would expect 3.3% of TRICARE's customers to experience some type of identity theft, even if the tapes were never read or misused. To quantify that percentage, of the 4.7 million customers whose data was on the tapes, one would expect around 155,100 of them to experience identity fraud simply by virtue of living in America and engaging in commerce, even if the tapes had not been lost. Here, only six Plaintiffs allege some form of identity theft, and out of those six only Curtis offers any plausible link to the tapes. And Yarde is the only other Plaintiff – out of a population of 4.7

million – who has offered any evidence that someone may have accessed her medical or personal information.

Given those numbers, it would be entirely implausible to assume that a massive identity-theft scheme is currently in progress or is certainly impending. Indeed, given that thirty-four months have elapsed, either the malefactors are extraordinarily patient or no mining of the tapes has occurred. This is simply not a case where hundreds or thousands of instances of fraud have been linked to the data breach. See, e.g., Anderson, 659 F.3d at 162-67. Rather, as far as the Court is aware, only six instances of fraud have been reported, and only two customers can plausibly link either identity theft or privacy violations to the tapes' loss. As such, only those two Plaintiffs whose harm is plausibly linked to the breach may move forward with their claims.

IV. Conclusion

Since the majority of Plaintiffs has been dismissed – potentially altering the scope of the remaining litigants' claims moving forward – the Court will pause to confer with the parties before determining which, if any, of the Complaint's twenty counts has been properly alleged. The Court thus reserves the issue of whether Defendants' Rule 12(b)(6) Motions should be granted for a future date. It further notes that it expects the parties to confer before the forthcoming status to determine if they can reach some agreement on the next procedural steps in the case.

For the aforementioned reasons, the Court will grant in part and deny in part Defendants' Motions to Dismiss. A separate Order consistent with this Opinion will be issued this day.

/s/ James E. Boasberg
JAMES E. BOASBERG
United States District Judge

Date: May 9, 2014