UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CHANTAL ATTIAS, et al., Plaintiffs, v. **CAREFIRST, INC., et al.**, Defendants.	Case No. 15-cv-00882 (CRC)

MEMORANDUM OPINION

Theft of electronic data has become commonplace in our digital economy, victimizing millions of Americans each year. But while the resulting harm to consumers can be catastrophic, not all data breaches result in legally actionable injuries. As a result, when consumers whose data has been compromised seek redress in the courts, it must be determined whether their alleged injuries are sufficiently specific and concrete to give them standing to sue. That is the task presently before the Court in this case.

In June 2014, the health insurer CareFirst suffered a data breach that compromised the personal information of some 1.1 million policyholders, including the seven named Plaintiffs here. The purloined information included the policyholders' names, birth dates, email addresses, and subscriber identification numbers. Compl. ¶ 32; see also Defs.' Reply Ex. 1 (Decl. Clayton Moore House) ¶ 10. According to CareFirst, more-sensitive data, such as social security and credit card numbers, was not stolen.[1] After CareFirst publicly acknowledged the breach in May

[1] Although Plaintiffs assert in their opposition to the motion to dismiss that their social security numbers were stolen in the data breach, the Complaint neither makes that allegation explicitly nor contains any factual contentions that would support that conclusion. See Pls.' Opp'n 17 (citing Compl. ¶ 57).

2015, Plaintiffs sued the company and various of its affiliates on behalf of themselves and other policyholders, alleging that CareFirst violated a host of state laws and legal duties by failing to safeguard their personal information.[2] Another set of plaintiffs filed a similar federal class action in Maryland.

CareFirst has moved to dismiss Plaintiffs' complaint. It argues that because Plaintiffs have not alleged that their personal information has actually been misused, or explained how the stolen information could readily be used to assume their identities, they lack standing to sue in federal court. Plaintiffs mainly respond that the increased likelihood of identity theft that resulted from the breach, and the costs they have incurred to mitigate it, are sufficient injuries to establish standing. In resolving this dispute, the Court will follow the standard set by the majority of courts that have confronted similar cases, including the related Maryland class action: Absent facts demonstrating a substantial risk that stolen data has been or will be misused in a harmful manner, merely having one's personal information stolen in a data breach is insufficient to establish standing to sue the entity from whom the information was taken. Because Plaintiffs have not made the required showing, the Court lacks subject matter jurisdiction over the case and will grant CareFirst's motion to dismiss.

I. Legal Standard

Defendants move to dismiss the Complaint for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1) and for failure to state a claim upon which

[2] Plaintiffs allege that the Court has jurisdiction over the case pursuant to 28 U.S.C. § 1332(d)(2) because the class's aggregate claims exceed $5,000,000 and "there are numerous class members who are citizens of states other than the Defendants." Compl. ¶ 10. The Court will not assess this assertion because, as discussed below, it will dismiss the case for lack of subject matter jurisdiction on standing grounds.

relief can be granted pursuant to Rule 12(b)(6). "The distinctions between 12(b)(1) and 12(b)(6) are important and well understood. Rule 12(b)(1) presents a threshold challenge to the court's jurisdiction, whereas 12(b)(6) presents a ruling on the merits with res judicata effect." Al-Owhali v. Ashcroft, 279 F. Supp. 2d 13, 20 (D.D.C. 2003) (quoting Haase v. Sessions, 835 F.2d 902, 906 (D.C.Cir.1987)) (internal quotation marks omitted). Because "a court must begin with questions of jurisdiction" "[b]efore examining the merits of any claim," In re Sci. Applications Int'l Corp. ("SAIC"), 45 F. Supp. 3d 14, 23 (D.D.C. 2014), and because the Court will conclude that it lacks subject matter jurisdiction, this Opinion will address only Defendants' jurisdictional arguments. Thus, "Federal Rule of Civil Procedure 12(b)(1) provides the relevant legal standard." Id. at 22. Under this standard, the Court must "treat the [C]omplaint's factual allegations as true . . . and must grant [Plaintiffs] the benefit of all inferences that can be derived from the facts alleged." Id. (omission in original) (quoting Sparrow v. United Air Lines, Inc., 216 F.3d 1111, 1113 (D.C. Cir. 2000)) (internal quotation marks omitted).

At the same time, because a "court has an 'affirmative obligation to ensure that it is acting within the scope of its jurisdictional authority,'" id. at 23 (quoting Grand Lodge of Fraternal Order of Police v. Ashcroft, 185 F. Supp. 2d 9, 13 (D.D.C. 2001)), a plaintiff'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. (quoting Grand Lodge, 185 F. Supp. 2d at 13–14) (internal quotation mark omitted). "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.'"[3] Id. (quoting Jerome Stevens Pharm. v. FDA, 402 F.3d 1249, 1253 (D.C. Cir. 2005)).

II. Analysis

Article III of the U.S. Constitution limits the reach of federal jurisdiction to the resolution of cases and controversies. See U.S. Const. art. III, § 2. "Because 'standing is an essential and unchanging part of the case-or-controversy requirement of Article III,'" SAIC, 45 F. Supp. 3d at 23 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)), "standing is a necessary 'predicate to any exercise of [the Court's] jurisdiction,'" id. (alteration in original) (quoting Fla. Audubon Soc'y v. Bentsen, 94 F.3d 658, 663 (D.C. Cir. 1996)). Consequently, every federal court plaintiff "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." Id. (quoting Dominguez v. UAL Corp., 666 F.3d 1359, 1362 (D.C. Cir. 2012)) (internal quotation marks omitted). "Even in the class-action context, all named Plaintiffs must allege and show that they *personally* have been injured." Id. (quoting Warth v. Seldin, 422 U.S. 490, 502 (1975)) (internal quotation mark omitted). And plaintiffs must plead or prove, "with the requisite 'degree of evidence required at the successive stages of the litigation,'" each element of standing. Id. (quoting Lujan, 504 U.S. at 561). Thus, "at the motion-to-dismiss stage, Plaintiffs must plead facts that, taken as true, make the existence of standing *plausible*." Id.

The question at issue here is whether the named Plaintiffs have demonstrated an "injury in fact" that is concrete, particularized, and actual or imminent, Lujan, 504 U.S. at 560 (quoting Allen v. Wright, 468 U.S. 737, 756 (1984)) (internal quotation marks omitted), and, if so,

[3] For this reason, the Court will consider, and deny, Plaintiffs' motion to strike the affidavit of CareFirst IT security official Clayton Moore House, which details the parameters of the data breach.

whether that injury is "fairly traceable" to the CareFirst data breach, id. at 590 (alteration omitted) (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41 (1976)) (internal quotation mark omitted). With the exception of two of the Plaintiffs—Kirk and Connie Tringler, who will be discussed below—none allege that they have suffered actual identity theft.[4] They contend instead that they have been harmed because the data breach has increased the likelihood that they will be the victims of identity theft in the future. In assessing such prospective harms, the Supreme Court held in Clapper v. Amnesty International USA that "[a]llegations of *possible* future injury" do not satisfy constitutional standing requirements. 133 S. Ct. 1138, 1147 (2013) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)) (internal quotation marks omitted). Rather, the "threatened injury must be *certainly impending* to constitute injury in fact." Id. (quoting Whitmore, 495 U.S. at 158) (internal quotation marks omitted). That does not mean that Plaintiffs are required to show that it is "literally certain that the harms they identify will come about." Id. at 1150 n.5. But they must at least demonstrate a "'substantial risk' that the

[4] Although the Plaintiffs' opposition to the Defendants' motion to dismiss asserts that "*many* Plaintiffs have already suffered identity theft, credit card fraud, and had their tax returns stolen," Pls.' Opp'n 5 (emphasis added) (citing Compl. ¶¶ 47–57), and that victims of the data breach other than the Tringlers have suffered "actual identity theft and fraud," id. at 3 (citing Compl. ¶ 57), the Complaint contains no factual allegations to support those assertions. The paragraphs of the Complaint Plaintiffs cite contain only conjecture regarding Plaintiffs other than the Tringlers. See Compl. ¶ 49 ("Identity thieves *can* use identifying data . . . to open new financial accounts and incur charges in another person's name . . . ." (emphasis added)); id. ¶ 50 ("Identity thieves *can* use personal information . . . to perpetrate a variety of crimes that do not cause financial loss, but nonetheless harm the victims. For instance, ..." (emphasis added)); id. ¶ 51 ("[I]dentity thieves *may* get medical services using the Plaintiff's PII [Personally Identifiable Information] and PHI [Personal Health Information] or commit any number of other frauds . . . ." (emphasis added)); id. ¶ 55 ("Identity thieves *can* use [stolen] information" to enroll unwilling beneficiaries into certain health plans. (emphasis added)). Because a "complaint may not be amended by the briefs in opposition to a motion to dismiss," BEG Invs., LLC v. Alberti, 85 F. Supp. 3d 13, 26 (D.D.C. 2015) (quoting Coleman v. Pension Benefit Guar. Corp., 94 F. Supp. 2d 18, 24 n.8 (D.D.C. 2000)) (internal quotation marks omitted), Plaintiffs' assertion of harm in their opposition does not constitute an allegation mounted in the Complaint.

harm will occur." Id. (quoting Monsanto Co. v. Geertson Seed Farms, 130 S. Ct. 2743, 2754–55 (2010)). Plaintiffs whose claim of injury depends on an "attenuated chain of inferences necessary to find harm" will "fall short" of the mark. Id. The Court turns to each of Plaintiffs' claimed injuries below.

A. Increased Risk of Identity Theft

Judge Boasberg of this Court recently applied Clapper's "certainly impending" standard to a claim of injury resulting from filched electronic data. SAIC, 45 F. Supp. 3d at 24. In that case, back-up tapes containing the personal information and medical records of military service members were among various items stolen from the car of an employee of the information technology company SAIC. See id. at 19–20. The data tapes originated with a federal agency that provides health insurance to military families, and SAIC was in possession of the tapes through an IT security contract with the agency. See id. Service members whose data was contained on the tapes sued, alleging in part that they had been harmed by the increased likelihood that they would suffer identity fraud as a result of the theft. See id.

The Court found the plaintiffs' claims of increased risk of identity theft to be insufficient to establish injury in fact. Judge Boasberg reasoned that too many assumptions were required to find the alleged harm certainly impending. The thief would still need to "recognize the tapes for what they were"; "find a tape reader and attach it to her computer"; "acquire software to upload the data"; decipher any encrypted portions of the data; "acquire familiarity with the [health insurance company's] database format, which might require another round of special software"; and finally, "either misuse a particular Plaintiff's [information] or sell that Plaintiff's data to a willing buyer who would then abuse it." Id. at 25. Because the plaintiffs had not alleged that

any of those things had occurred, and because those "events [were] entirely dependent on the actions of an unknown third party," they failed to demonstrate standing under Clapper. Id.

Plaintiffs attempt to distinguish SAIC by pointing out that, unlike the thieves there—who stole various physical objects from a car, some of which happened to contain data—those here breached CareFirst's server protections for the very purpose of accessing that data, thus demonstrating their intent to misuse it. See Pls.' Opp'n 10–11. Plaintiffs point to the Seventh Circuit's recent decision in Remijas v. Neiman Marcus Group, 794 F.3d 688 (7th Cir. 2015), as more-analogous precedent. Remijas involved a data breach of Neiman Marcus's computer systems, which compromised customers' credit card information, social security numbers, and birth dates. See id. at 690. Of the 350,000 credit cards whose information was potentially exposed, 9,200 "were known to have been used fraudulently." Id. In other words, the hackers had clearly demonstrated that they had the means and the will either to abuse the information they accessed or to sell it to others who did so. Unlike in SAIC, where only two plaintiffs out of the 4.7 million service members whose information was stolen plausibly alleged an injury traceable to the theft, SAIC, 45 F. Supp. 3d at 31–33, in Remijas, even the plaintiffs who had not yet experienced fraud had demonstrated that they faced a "substantial risk" of fraud sufficient to confer standing because so many other plaintiffs had experienced cognizable harm traceable to the breach, Remijas, 794 F.3d at 693.

The Court views SAIC to be more similar to this case than Remijas and other data breach cases cited by Plaintiffs. See Pls.' Opp'n 6–10. While the series of assumptions required to find concrete harm to Plaintiffs may be somewhat shorter here than that in SAIC, their theory of injury is still too speculative to satisfy Clapper. The Court would have to assume, at a minimum, that the hackers have the ability to read and understand Plaintiffs' personal information, the

intent to "commit future criminal acts by misusing the information," and the ability to "use such information to the detriment of [Plaintiffs] by making unauthorized transactions in [Plaintiffs'] names." Chambliss v. CareFirst, Inc., No. RDB-15-2288, 2016 WL 3055299, at *4 (D. Md. May 27, 2016) (alterations in original) (quoting In re SuperValu, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2586, 2016 WL 81792, at *5 (D. Minn. Jan. 7, 2016)) (internal quotation mark omitted). And, even more speculative than in SAIC—where social security numbers were among the stolen data—is the question whether the hackers here would be willing or able to use the existing data to acquire *additional* data. Plaintiffs have not suggested, let alone demonstrated, how the CareFirst hackers could steal their identities without access to their social security or credit card numbers. See, e.g., Antman v. Uber Techs., Inc., No. 3:15-cv-01175, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) ("[T]he court holds that Mr. Antman's allegations are not sufficient because his complaint alleges only the theft of names and driver's licenses. Without a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury."). The absence of such a showing distinguishes this case from Remijas, where the demonstrated existence of thousands of unauthorized charges shortly following the data breach clearly established a connection between the breach and the thieves' ability and willingness to commit fraud.

The court in the related Maryland class action reached same conclusion, granting the defendants' motion to dismiss for lack of subject matter jurisdiction on standing grounds. It rejected the plaintiffs' argument that the breach increased their risk of future harm because "most courts to consider the issue 'have agreed that the mere loss of data—without any evidence that it has been either viewed or misused—does not constitute an injury sufficient to confer standing.'"

Chambliss, 2016 WL 3055299, at *4 (quoting SAIC, 45 F. Supp. 3d at 19) (citing In re Zappos.com, Inc., 108 F.Supp.3d 949, 958–59 (D. Nev. 2015); Green v. eBay, Inc., No. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015); In re Horizon Healthcare Servs., Inc. Data Breach Litig., No. 13-7418, 2015 WL 1472483, at *6 (D.N.J. Mar. 31, 2015); Key v. DSW, Inc., 454 F.Supp.2d 684, 689 (S.D. Ohio 2006)). The court added that "since Clapper[,] . . . courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases." Id. (quoting SAIC, 45 F.Supp.3d at 28) (citing In re SuperValu, 2016 WL 81792, at *4); Strautins v. Trustwave Holdings, Inc., 27 F.Supp.3d 871, 876 (N.D. Ill. 2014)) (internal quotation marks omitted). This Court likewise concludes that Plaintiffs have not demonstrated a sufficiently substantial risk of future harm stemming from the breach to establish standing.

B. Actual Identity Theft

As noted above, two of the named Plaintiffs—Kirk and Connie Tringler—allege that they have already suffered an injury from the data breach. They claim that they have experienced tax-refund fraud in that they have still not received an expected tax refund. See Compl. ¶ 57. While suffering this type of fraud may constitute a concrete and particularized injury, in order to demonstrate standing, Plaintiffs must also plausibly assert that their alleged injury is "fairly traceable to the challenged action." Clapper, 133 S. Ct. at 1147. And again, while the Plaintiffs' opposition asserts that the stolen information included social security numbers, the Complaint does not support that allegation. See supra note 1; Pls.' Opp'n 17; Compl. ¶ 57. As Defendants point out, and Plaintiffs do not contest, "[i]t is not plausible that tax refund fraud could have been conducted without the Tringlers' Social Security Numbers." Defs. Reply 5; see also Furlow v. United States, 55 F. Supp. 2d 360, 362–63 (D. Md. 1999) ("[T]o receive an income tax exemption . . . , the taxpayer must include the social security number or taxpayer identification

number of the claimed individual on his returns."). Therefore, the Tringlers have not plausibly alleged that any tax-return fraud they have experienced is fairly traceable to the data breach.

C. Other Claimed Harms

In addition to arguing that the increased risk of future harm confers standing upon Plaintiffs other than the Tringlers and that the Tringlers have already experienced cognizable injury, all Plaintiffs contend that they have experienced four other types of harm: (1) economic harm through having to purchase credit-monitoring services to prevent identity theft and fraud; (2) economic harm through overpayment for their insurance coverage, the cost of which they maintain should have covered prophylactic measures against hacking; (3) loss of the intrinsic value of their personal information; and (4) violation of their statutory rights under consumer protection acts. None of the arguments in support of these contentions is availing.

First, because the increased risk of future identity theft or fraud is too speculative to confer standing, Plaintiffs cannot opt in to standing-conferring economic injury by purchasing protection from that future harm. Where "future harm . . . is not certainly impending," plaintiffs "cannot manufacture standing by choosing to make expenditures based on" that "hypothetical" harm. Clapper, 133 S. Ct. at 1143. In other words, Plaintiffs "cannot create standing by 'inflicting harm on themselves'" in the form of purchasing credit-monitoring services in order "to ward off an otherwise speculative injury." SAIC, 45 F. Supp. 3d at 26 (quoting Clapper, 133 S. Ct. at 1151).

Second, a claim that "some indeterminate part of their premiums went toward paying for security measures . . . is too flimsy to support standing." Id. at 30. Like the plaintiffs in SAIC, Plaintiffs here "do not maintain that the money they paid could have or would have bought a better policy with a more bullet-proof information-security regime." Id. Nor have they "alleged

facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid." Id.

Third, also like the plaintiffs in SAIC, "Plaintiffs do not contend that *they* intended to sell [their personal] information on the cyber black market in the first place, so it is uncertain how they were injured" by the alleged loss of the intrinsic value of that information. Id. In addition, "it is unclear whether or how the data has been devalued by the breach." Id. Without factual allegations to support this contention, Plaintiffs do not plausibly assert harm from the loss of their personal information's intrinsic value.

Fourth, Plaintiffs contend that this Court must conclude that they have standing because the D.C. Court of Appeals, they assert, has held that a violation of the D.C. Consumer Protection Procedures Act can confer standing on its own. See Pls.' Opp'n 13 (citing Grayson v. AT&T Corp., 15 A.3d 219, 247 (D.C. 2011)). Setting aside the fact that only the Plaintiffs who are residents of the District of Columbia assert violations of this D.C. Act, statutory rights cannot confer Article III standing on a plaintiff who does not have it otherwise. See Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547–48 (2016) ("Injury in fact is a constitutional requirement, and '[i]t is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.'" (alteration in original) (quoting Raines v. Byrd, 521 U.S. 811, 820 n.3 (1997))). This is so because an injury in fact must be "both 'concrete *and* particularized.'" Id. at 1545 (quoting Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000)). While violation of a plaintiff's statutory rights is not irrelevant to standing, it is also not sufficient because it "concern[s] particularization, not concreteness," id. at 1548: "Article III standing requires a concrete injury even in the context of a statutory violation," id. at 1549. And a "'concrete' injury

must be '*de facto*'; that is, it must actually exist." Id. at 1548. Where a violation of a statute "may result in no harm," that mere violation is insufficient to confer standing. Id. at 1550. Even if Plaintiffs' rights under applicable consumer protection acts have been violated, because they do not plausibly allege concrete harm, they have not demonstrated that they have standing to press their claims.[5]

III. Conclusion

For the foregoing reasons, Defendants' motion to dismiss will be granted and the Second Amended Complaint dismissed without prejudice, and Plaintiffs' motion to strike will be denied. An order accompanies this memorandum opinion.

CHRISTOPHER R. COOPER
United States District Judge

Date: August 10, 2016

[5] Plaintiffs have filed a notice of supplemental authority flagging for the Court a recently decided D.C. Circuit case concerning an alleged violation of D.C. laws protecting consumers from the disclosure of contact information in the course of credit card transactions. See Hancock v. Urban Outfitters, Inc., No. 14-7047, 2016 WL 3996710 (D.C. Cir. July 26, 2016). The court held that the plaintiffs failed to establish standing because, although they alleged statutory violations, they did not allege any concrete injury in fact as a result of those violations. See id. at *6–7. In dicta, the court noted that "increased risk of fraud or identity theft . . . may satisfy Article III's requirement of concrete injury." Id. at *7. It is this statement that Plaintiffs emphasize in their notice. However, the D.C. Circuit's reasoning, and the principal that increased risk of harm *may* satisfy the constitutional requirement of concrete injury are entirely consistent with the Court's analysis here.