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

Plaintiffs brought this putative class action against D.C.-area health insurer CareFirst and various of its affiliates after CareFirst suffered a data breach in 2014. The breach compromised the names, birthdates, email addresses, and subscriber identification numbers of over one million of CareFirst's insureds. The named plaintiffs are seven of those insureds, and they lodge a host of contract, tort, and state-specific statutory claims against the company stemming from the breach.

CareFirst has now twice moved to dismiss the complaint. On the first occasion, the Court granted the motion on standing grounds and dismissed the complaint in its entirety. That decision was reversed by the D.C. Circuit, which concluded that plaintiffs' heightened risk of future identity theft satisfied the injury-in-fact requirement of Article III standing. On remand, CareFirst renewed its motion to dismiss the complaint for failure to state a claim, which the Court granted in substantial part. All told, the Court dismissed all the claims in the complaint save two claims advanced by the two named plaintiffs who alleged actual misuse of their exposed data. The Court then issued a final order as to the dismissed claims under Federal Rule of Civil Procedure 54(b), thereby permitting plaintiffs to appeal. However, the D.C. Circuit

concluded that the requirements of Rule 54(b) had not been met and thus dismissed the appeal for lack of jurisdiction.

Following remand, plaintiffs filed the present motion for reconsideration of the Court's dismissal of their claims under Rule 12(b)(6). Reconsideration is warranted, plaintiffs argue, to clarify that D.C. law does not require actual damages to sustain a breach of contract claim; to address intervening D.C. Circuit precedent that, in plaintiffs' view, widens the scope of "actual damages" stemming from the data breach; and to correct the Court's prior analysis of the relationship between plaintiffs' claims under the District of Columbia Consumer Protection Procedures Act and their breach of contract claims. For the following reasons, the Court will grant the motion in part and deny it in part.

I. Background

A. Factual Background

The Court presumes familiarity with its two prior opinions, Attias v. CareFirst, Inc., 199 F. Supp. 3d 193 (D.D.C. 2016) ("Attias I"), and Attias v. CareFirst, Inc., 365 F. Supp. 3d 1 (D.D.C. 2019) ("Attias II"), which fully recount the background facts. The Court will only briefly summarize them here.

CareFirst, Inc. and certain of its affiliates (collectively, "CareFirst") operate a group of health insurance companies that provide coverage to over one million people in the District of Columbia, Maryland, and Virginia. See Second Am. Class Action Compl., ¶ 23 ("SAC") ECF No. 9. To receive CareFirst insurance, customers provide the company with personal information including their names, addresses, and social security numbers. Id. ¶¶ 26–27. In June 2014, this information (with the exception, according to CareFirst, of the insureds' social security numbers) was compromised when the company suffered a data breach. Id. ¶ 33.

CareFirst discovered the breach in April 2015 and notified the public the following month. Id. ¶ 15, 35–36. Shortly thereafter, plaintiffs filed this putative class action.

B. Procedural Background

1. The complaint

The operative complaint names seven plaintiffs: Chantal Attias and Andreas Kotzur of the District of Columbia, Richard and Latanya Bailey of Virginia, and Curt and Connie Tringler and Lisa Huber of Maryland. Id. ¶¶ 1–4. They each allege that CareFirst's carelessness in handling their personal information violated D.C. tort and contract laws, as well as the consumer protection statutes of each plaintiff's home state. All told, the complaint contains eleven claims: breach of contract (Count I), negligence (Count II), violation of the District of Columbia Consumer Protection Procedures Act ("CPPA") (Count III), violation of the District of Columbia Data Breach Notification Act (Count IV), violation of the Maryland Consumer Protection Act ("MCPA") (Count V), violation of the Virginia Consumer Protection Act ("VCPA") (Count VI), fraud (Count VII), negligence *per se* (Count VIII), unjust enrichment (Count IX), breach of the duty of confidentiality (Count X), and constructive fraud (Count XI).

By way of damages, plaintiffs allege that the data breach heightened their risk of future identity theft, resulting in "economic and non-economic loss in the form of mental and emotional pain and suffering," id. ¶ 38, as well as "years of constant surveillance of their financial and personal records, monitoring, and loss of rights," id. ¶ 56. Two plaintiffs, the Baileys of Virginia, also allege that "they were not given the benefit of the services for which they bargained[.]" Id. ¶ 114. Two more plaintiffs, the Tringlers of Maryland, allege that they suffered "tax-refund fraud" because, at least at the time of the complaint, they had not received an expected federal tax refund. Id. ¶ 57.

2. Dismissal for lack of jurisdiction

In September 2015, CareFirst moved to dismiss the complaint for lack of subject matter jurisdiction under Rule 12(b)(1) and for failure to state a claim under Rule 12(b)(6). See Mot. to Dismiss, ECF No. 13. The Court granted the Rule 12(b)(1) motion, finding that it lacked subject matter jurisdiction because plaintiffs failed to satisfy the injury-in-fact requirement of Article III standing. See Attias I, 199 F. Supp. 3d at 203. Five of the seven plaintiffs (all but the Tringlers) failed to allege any actual misuse of their information. In accord with several other district court decisions nationwide—including one dismissing a Maryland federal class action brought by another group of CareFirst customers affected by the same breach—the Court concluded that "merely having one's personal information stolen in a data breach is insufficient to establish standing to sue the entity from wh[ich] the information was taken." Id. at 197. As to the Tringlers, the Court found that they failed to plausibly allege either (i) that their social security numbers were stolen as part of the breach, or (ii) that tax refund fraud could occur without the perpetrators having access to such numbers. Id. at 201. The Court therefore concluded that the Tringlers' injury was not "fairly traceable" to the breach and that they, too, lacked standing. Id. (citing Clapper v. Amnesty Int'l, 568 U.S. 398, 409 (2013)).

The D.C. Circuit reversed. See Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017). The court reasoned that the complaint contained specific allegations that CareFirst "collected and stored" personal information that could be combined to commit identity theft and fraud—even if the compromised information did not include plaintiffs' social security numbers. Id. at 628. The resulting "risk of future injury" was alone "substantial enough to create Article III standing." Id.

3. Dismissal for failure to state a claim

On remand, CareFirst filed a renewed Rule 12(b)(6) motion to dismiss for failure to state a claim. See Mot. to Dismiss, ECF No. 44. The Court granted the motion in substantial part, permitting only two claims brought by the Tringlers to proceed. See Attias II, 365 F. Supp. 3d 1 (D.D.C. 2019). As that opinion is the basis of the present motion for reconsideration, the Court will describe it in some detail.

In resolving CareFirst's renewed motion, the Court began by addressing the company's argument that plaintiffs failed to plead actual damages as required by nine of the eleven claims—specifically, those for (1) breach of contract, (2) negligence, (3) negligence *per se*, (4) fraud, (5) constructive fraud, (6) breach of duty of confidentiality, (7) violation of the MCPA, (8) violation of the VCPA, and (9) violation of the D.C. Data Breach Notification Act. The Court addressed each claim under the relevant governing law (for the most part, D.C. common law) and concluded that each required an allegation of actual damages.

Turning to the operative complaint, the Court observed four potential theories of damages: (1) actual misuse of personal information, (2) benefit of the bargain struck in the underlying insurance contracts, (3) mitigation costs, and (4) emotional distress. Starting from the top, the Court concluded that "actual misuse" of exposed information clearly qualified as "actual damages." Attias II, 365 F. Supp. 3d at 11–12. It stressed, however, that under the D.C. Court of Appeals' decision in Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 708 (D.C. 2009), actual misuse of personal data under D.C law requires more than a mere *threat* of future misuse. Rather, to sufficiently plead actual damages under that theory, D.C. common law requires the plaintiff to allege an instance of present (or actual) misuse of her personal data. See id. Only the Tringlers, who alleged that they suffered tax refund fraud as a result of the breach,

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.