ATTIAS et al v. CAREFIRST, INC. et al Doc. 107

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CHANTAL ATTIAS, et al., Plaintiffs, v. **CAREFIRST, INC., et al.**, Defendants.	Case No. 15-cv-882 (CRC)

MEMORANDUM OPINION AND ORDER

In April 2014, a cyberattack executed through an email spear phishing campaign gave hackers unauthorized access to the internal computer systems of Defendant CareFirst, Inc., a health insurance company. Unbeknownst to CareFirst, the hackers secretly remained on the company's systems for months, eventually exfiltrating certain personal identifying information of CareFirst's customers. With the help of an outside investigation, CareFirst eventually uncovered the mischief, but it was too late to stop the breach. Plaintiffs in this case, a group of those customers whose information was exposed in the breach, filed a class action lawsuit against CareFirst. Eight years, several motions, and thousands of documents later, only three of Plaintiffs' claims remain. CareFirst now has filed a motion for summary judgment on those claims, which are for breach of contract and violations of consumer protection statutes in both Maryland and Virginia.

For the reasons detailed in this opinion, the Court will deny CareFirst's motion as to Plaintiffs' breach of contract claim but will grant summary judgment for CareFirst as to the Maryland and Virginia consumer protection claims. Although the evidence on which Plaintiffs rely is thin, the Court finds that a reasonable jury could conclude that CareFirst breached an implied promise to take reasonable steps to safeguard their personal information. Under the

Dockets.Justia.com

Maryland Consumer Protection Act, however, Plaintiffs have failed to show a triable issue of fact on a key element—reliance on CareFirst's alleged misrepresentations about the company's data security practices. And Plaintiff's Virginia Consumer Protection Act claim is foreclosed because CareFirst falls within an exemption in the statute for insurance companies regulated by the state's corporation commission.

I. Background

Plaintiffs are District of Columbia, Maryland, and Virginia residents who had health insurance provided by Defendant CareFirst, Inc.[1] during the time relevant to this lawsuit. In April 2014, hackers gained access into CareFirst's computer system through an email-based spear phishing campaign, using an email designed to resemble an official message from CareFirst. The email was targeted to reach 48 CareFirst employees. Mot. for Summ. J. ("MSJ"), Ex. Q at 3; MSJ, Ex. C at 105–06. About half a dozen CareFirst employees accessed a malicious URL linked in the email, and five downloaded and ran the malicious software accessed via the link. MSJ, Ex. Q at 3. CareFirst took immediate steps to remedy the hacking attempt, including resetting those employees' passwords and taking their computers offline, examining the computers, and reimaging them. MSJ, Ex. C at 193–94; MSJ, Ex. Q at 3–4. But another CareFirst Employee, Wesley Doyle, who worked in the IT department and had special administrator credentials which provided deeper access into CareFirst's computers, also clicked on the malicious link and thereby gave the hackers broader, undetected access to CareFirst's systems. MSJ, Ex. A (Moore Decl.) ¶ 15. Doyle told CareFirst that he was not using his

[1] Defendants in this case include various related corporate entities—CareFirst, Inc., Group Hospitalization and Medical Services, Inc., CareFirst of Maryland, Inc., and CareFirst Bluechoice. See Second Amended Compl. ("SAC") ¶¶ 5–8. Unless otherwise indicated, the Court will refer to all these entities collectively as "CareFirst."

administrator account when he clicked the malware link, but it turned out that the hackers nonetheless gained administrator credentials. Id.; MSJ, Ex. C at 141–49, 164–69.

Sometime after the April incident, in light of reports from other Blue Cross licensees Anthem and Premera that their computer systems had been attacked, CareFirst retained external counsel and hired a cybersecurity firm, Mandiant, to conduct a forensic investigation into whether CareFirst had also been attacked. Defendants' Statement of Undisputed Facts ("DSUF") ¶¶ 37–39. Mandiant conducted an assessment between March 20, 2015 and May 4, 2015 and, on its 70th and final scan of the CareFirst computer systems, detected evidence that CareFirst's systems had been compromised by hackers. Id. ¶¶ 41–42.

As discussed further below, Plaintiffs maintain that CareFirst and its employees committed several errors that allowed the hackers to gain access to CareFirst's systems, to remain in those systems undetected, and to purloin certain personally identifying information ("PII") of CareFirst customers. SAC ¶¶ 64–75. Specifically, due to the breach, hackers accessed a database containing the following information of Plaintiffs and the class they seek to represent: their names, subscriber ID numbers, dates of birth, e-mail addresses, and usernames chosen for access to CareFirst's online member portal (but not their Social Security numbers or any financial information). MSJ at 4; DSUF ¶ 2; MSJ, Ex. Q at 4; SAC ¶ 94. The breach of this information affected more than one million CareFirst customers. MSJ at 4; DSUF ¶ 1. After discovering the exfiltration of this data, in May 2015, CareFirst sent letters to members whose PII might have been affected, notifying them of the data breach, advising them to reset their online portal credentials, and offering them two years of free credit monitoring and identity theft protection services through an Experian product called ProtectMyID. MSJ, Ex. R.

A few weeks later, in June 2015, Plaintiffs brought this class action lawsuit, originally consisting of eleven claims including breach of contract, negligence, violation of D.C., Maryland, and Virginia consumer protection laws, violation of the D.C. Data Breach Notification Act, negligence *per se*, unjust enrichment, breach of duty of confidentiality, fraud, and constructive fraud. SAC ¶¶ 64–154. As relevant here, Plaintiffs' breach of contract claims are premised on the privacy statements contained in CareFirst's health insurance agreements, which provided, with some variation, that CareFirst would "comply with State, Federal and local laws pertaining to the dissemination or distribution of non-public personally identifiable medical or health-related data" and, to that end, would "not provide . . . unauthorized third parties any personally identifiable medical information without the prior written authorization of the patient." DSUF ¶¶ 13, 17, 20, 24; MSJ, Ex. B ¶¶ 18, 22, 25, 29. Plaintiffs' Maryland and Virginia consumer protection act claims are premised on CareFirst's Notice of Privacy Practices—a document describing the company's privacy policies and practices to consumers—which stated, among other things, that CareFirst "maintain[ed] physical, electronic and procedural safeguards in accordance with federal and state standards to protect your health information." MSJ, Ex. Z at 1.

In 2016, the Court dismissed the case for lack of standing, explaining that Plaintiffs' theory of injury was too speculative. The D.C. Circuit reversed, holding that Plaintiffs had pleaded that information such as credit card and Social Security numbers had been accessed and that, even if the breached data was more limited, Plaintiffs had pleaded a risk of "'medical identity theft,' in which a fraudster impersonates the victim and obtains medical services in her name." Attias v. Carefirst, Inc. (Attias I), 865 F.3d 620, 627–29 (D.C. Cir. 2017). On remand, the Court dismissed for failure to state a claim all causes of action except for the breach of

contract and Maryland Consumer Protection Act ("MCPA") claims brought by Plaintiffs Curt and Connie Tringler. Attias v. CareFirst, Inc. (Attias II), 365 F. Supp. 3d 1 (D.D.C. 2019). As relevant here, the Court concluded that all Plaintiffs except the Tringlers had failed adequately to allege actual damages as required for most of their claims. Id. at 27.

After Plaintiffs filed a motion for reconsideration, the Court reinstated the breach of contract claim as to all Plaintiffs. Attias v. CareFirst, Inc. (Attias III), 518 F. Supp. 3d 43 (D.D.C. 2021). The Court observed that, although there is some D.C. Court of Appeals authority suggesting that actual damages are required for a prima facie contract claim, other authority, which had not been provided to the Court previously, holds that "'[e]ven where monetary damages cannot be proved' the prevailing party may be entitled to nominal damages, specific performance, or declaratory relief." Attias III, 518 F. Supp. 3d at 52 (quoting Wright v. Allen, 60 A.3d 749, 753 & n.3 (D.C. 2013)). However, the Court rejected Plaintiffs' argument that money spent to mitigate against potential future identity theft or fraud constituted "actual damages" under D.C. law. Id. at 52–55. The Court also reinstated Plaintiffs' claims under the MCPA and Virginia Consumer Protection Act ("VCPA"). Id. at 57. The Court observed that, although the Virginia statute requires a "loss" for Plaintiffs to recover, the law also permits recovery of a $500 civil penalty when actual damages are *de minimis*, and Virginia courts have read those loss and actual damages requirements expansively. Id. at 55–56. Although the Maryland statute is more restrictive than the Virginia act, the Court held that absent any binding authority to the contrary, "the D.C. Circuit, consistent with its reasoning in [In re: U.S. Office of Personnel Management Data Security Breach Litigation, 928 F.3d 42 (D.C. Cir. 2019)], would

be more likely than not to treat mitigation expenses as actual damages under both statutes." Id. at 56.[2]

CareFirst now moves for summary judgment as to Plaintiffs' breach of contract, MCPA, and VCPA claims.

II. Legal Standards

The Court should grant summary judgment "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A genuine issue of material fact exists if the evidence is "'such that a reasonable jury could return a verdict for the nonmoving party,' resolving all ambiguities and drawing all factual inferences in favor of the nonmoving party." Moore v. Hartman, 571 F.3d 62, 66 (D.C. Cir. 2009) (quoting Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986)). The moving party "bears the initial responsibility of informing the district court of the basis for its motion, and identifying those portions of the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, which it believes demonstrate the absence of a genuine issue of material fact." Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986) (internal quotation marks omitted). The nonmoving party must then "designate specific facts showing that there is a genuine issue for trial." Id. (internal quotation marks omitted). A dispute is "genuine" only if a reasonable jury could find for the nonmoving party, and a fact is "material" only if "it is capable of affecting the outcome of the litigation." Egudu v. District of Columbia, 72 F. Supp. 3d 34, 40 (D.D.C. 2014) (citing Liberty Lobby, 477 U.S. at

[2] A few months ago, the Court denied without prejudice to renewal Plaintiffs' motion for class certification, largely based on concerns about class-member standing and individualized reliance determinations as to Plaintiffs' MCPA and VCPA claims. Plaintiffs have filed a renewed motion for class certification, which the Court does not address in this opinion.

248). When reviewing a summary judgment motion, the Court must "view the facts and draw reasonable inferences 'in the light most favorable to the party opposing the'" motion. Scott v. Harris, 550 U.S. 372, 378 (2007) (quoting United States v. Diebold, Inc., 369 U.S. 654, 655 (1962)). "Credibility determinations, the weighing of the evidence, and the drawing of legitimate inferences from the facts are jury functions" and thus not appropriate exercises for "a judge at summary judgment." Barnett v. PA Consulting Grp., Inc., 715 F.3d 354, 358 (D.C. Cir. 2013) (quoting Pardo–Kronemann v. Donovan, 601 F.3d 599, 604 (D.C. Cir. 2010)).

III. Analysis

The Court begins with Plaintiffs' breach of contract claims. Although Plaintiffs' theories of contract liability are somewhat underdeveloped, and the evidence supporting their claim is thin, the Court concludes that summary judgment is inappropriate as to at least one of their theories—that CareFirst violated an implied contractual duty to take reasonable steps to secure Plaintiffs' PII by failing to take certain security measures at the time of the data breach. Thus, the Court will deny the summary judgment motion as to Plaintiffs' breach of contract claim. The Court will grant CareFirst's motion for summary judgment as to the MCPA and VCPA claims, however. As for the former claim, Plaintiffs have failed to produce evidence from which a reasonable jury could find that Plaintiffs relied on CareFirst's statements about data security in the Notice of Privacy Practices. As to the latter claim, CareFirst falls outside the scope of the VCPA, which exempts from its coverage insurance companies, including CareFirst, that are regulated by Virginia's State Corporation Commission.

A. Breach of Contract

"To prevail on a claim of breach of contract, a party must establish (1) a valid contract between the parties; (2) an obligation or duty arising out of the contract; (3) a breach of that duty;

and (4) damages caused by breach." Francis v. Rehman, 110 A.3d 615, 620 (D.C. 2015) (emphasis omitted) (quoting Tsintolas Realty Co. v. Mendez, 984 A.2d 181, 187 (D.C. 2009)). As to duty and breach, CareFirst maintains that, to the extent the privacy statements in CareFirst's insurance plans with Plaintiffs imposed a duty to "comply with state, federal and local laws pertaining to the dissemination or distribution" of PII and a duty not to provide unauthorized third parties with any member PII, this duty pertains only to affirmative dissemination of PII, not hacking by unauthorized third parties. MSJ at 9–12. CareFirst thus contends that it complied with this duty because it did not freely disseminate PPI. Id. Second, to the extent Plaintiffs' contract claim is premised on a promise to abide by the Health Insurance Portability and Accountability Act ("HIPAA"), CareFirst maintains that it "safeguarded Plaintiffs' [PII] in accordance with HIPAA," citing, for instance, a 2013 privacy and security risk audit by KPMG that found CareFirst had robust security systems. Id. at 12–14. Third, CareFirst argues that any breach was not material. Id. at 17. Last, CareFirst renews arguments previously presented to the Court that Plaintiffs have no actual damages and that any nominal damages are *de minimis*. Id. at 15–18.[3] The Court addresses each of these arguments, and Plaintiffs' responses, in turn.

1. Contractual Duties

CareFirst concedes that its relationship with the Plaintiffs was contractual but contends that the only contractual duty arising from the Privacy Statements in Plaintiffs' insurance agreements was a duty not to affirmatively disseminate, distribute, or provide Plaintiffs' PII to unauthorized persons. MSJ at 11. Although their briefing is less than clear at times, Plaintiffs

[3] CareFirst also asserts that two of the named Defendants—CareFirst, Inc. and Group Hospitalization and Medical Services, Inc.—had no contractual relationship with any Plaintiffs, a contention Plaintiffs do not dispute. MSJ at 9 n.2; Reply at 2 n.2.

appear to articulate two different theories of CareFirst's contractual duties: (1) an *express* promise in the CareFirst Privacy Statements to comply with federal law, and HIPAA in particular, in protecting member PII, Opp'n at 12–14, and (2) an *implied* promise to "use adequate [or reasonable] measures to safeguard Plaintiffs'" PII, evidenced in part by representations made in CareFirst's Notice of Privacy Practices, id. at 6–7. The Court begins by addressing whether the express terms of CareFirst's Privacy Statements imposed only an obligation for the company not to affirmatively disseminate customer PII to unauthorized parties or also created a duty to prevent malicious third-party hackers from gaining access to PII, specifically by virtue of the contracts' reference to compliance with state, federal, and local laws regarding the distribution of PII.[4]

In relevant part, CareFirst's Privacy Statements provide that the company "shall comply with state, federal and local laws pertaining to the dissemination or distribution of non-public personally identifiable financial, medical or health related data" and, "[i]n that regard," the company "will not provide to . . . unauthorized third parties any personally identifiable financial

[4] As a preliminary matter, CareFirst maintains that "Plaintiffs disavowed reliance on alleged HIPAA violations for all but their negligence *per se* claim, which the Court dismissed" at the motion to dismiss stage. MSJ at 13. The Court disagrees. In their opposition to CareFirst's Rule 12(b)(6) motion to dismiss, Plaintiffs stated that "only Plaintiffs' Negligence *per se* cause of action requires a finding that HIPAA was violated to be plausibly stated." Opp. to Mot. to Dismiss at 19, ECF No. 45. In context, however, the Court understands this statement to express only Plaintiffs' position that their other claims could survive even without finding a HIPAA violation. The opposition went on to say that Plaintiffs' "breach of contract claim listed several terms other than HIPAA violations which were breached." Id. Although the Court's opinion on the motion to dismiss observed in a footnote that Plaintiffs "disavowed reliance on alleged HIPAA violations for all but their negligence *per se* claim," Attias II, 365 F. Supp. 3d at 25 n.17, in context, this observation simply described Plaintiffs' opposition and did not purport to bar any future reliance on a HIPAA-violation theory, which is expressly raised in Plaintiffs' complaint. See SAC ¶¶ 68–69. Additionally, although CareFirst also points out that HIPAA does not provide a private right of action, MSJ at 12, the Court sees no reason why that fact would preclude a breach of contract claim premised on the violation of a promise to maintain HIPAA-compliant security systems.

or medical information without the prior written authorization of the patient or parent/guardian of the patient or as otherwise permitted by law." MSJ, Ex. B ¶ 25.[5] CareFirst contends that this promise pertains only to CareFirst's *affirmative* "dissemination," "distribution," or "provi[sion]" of sensitive PII to unauthorized third parties and, therefore, does not cover the conduct at issue here—a hacker gaining unauthorized access into CareFirst's computers despite CareFirst's security measures. MSJ at 11–12; Reply at 2. Because there is no evidence that CareFirst intentionally provided PII to outside parties, CareFirst maintains summary judgment is warranted. To this argument, Plaintiffs respond, albeit without any elaboration, that the terms "dissemination," "distribution," and "provide" are ambiguous, rendering summary judgment inappropriate under D.C. law. See Plaintiffs' Statement of Material Facts ("PSMF") ¶ 10 ("[T]he ambiguous nature of the words 'affirmatively,' 'disseminate,' 'distribute,' and 'provide' are open to interpretation and therefore create a genuine dispute of material fact."); Aziken v. District of Columbia, 70 A.3d 213, 219 (D.C. 2013) (summary judgment improper where contract terms are ambiguous).

The Court agrees with CareFirst that this particular language created a limited obligation on CareFirst to comply with applicable law with regard to its affirmative disclosure of PII. As CareFirst points out, the terms "dissemination," "distribution," and "provide" all speak to CareFirst's affirmative conduct, e.g., its policies concerning when it may share private medical information with health care providers or employers. See Disseminate, Merriam-Webster, https://www.merriam-webster.com/dictionary/disseminate (last visited Sept. 13, 2023) ("to spread abroad as though sowing seed; to disperse throughout"); Distribute, Merriam-Webster,

[5] The Privacy Statements in Plaintiffs Richard and Latanya Bailey's agreement do not include this express term, promising only to "keep your medical and claims records confidential." Id. ¶ 29.

https://www.merriam-webster.com/dictionary/distribute (last visited Sept. 13, 2023) ("to spread out so as to cover something; to give out or deliver especially to members of a group"); Provide, Merriam-Webster, https://www.merriam-webster.com/dictionary/provide (last visited Sept. 13, 2023) ("to supply or make available (something wanted or needed); to make something available to"). This language stands in contrast to the broader language of CareFirst's Notice of Privacy Practices (on which Plaintiffs do not appear to rely for any express contract argument), which promises that the company "maintain[s] physical, electronic and procedural *safeguards* in accordance with federal and state standards to *protect* your health information." MSJ, Ex. Z at 1 (emphasis added). Unlike the insurance agreements, the Notice of Privacy Practices seems to describe an affirmative duty to "protect" or "safeguard" information, as opposed to a duty merely not to "disclose" or "disseminate" it without authorization.

As to Plaintiffs' implied contractual term theory, however, the Court agrees that their contracts with CareFirst included an implicit promise to take reasonable steps to secure their PII against unauthorized intrusion by third parties. "Under D.C. law, an implied-in-fact contract contains 'all necessary elements of a binding agreement,' differing from other contracts 'only in that it has not been committed to writing' and is instead 'inferred from the conduct of the parties.'" Camara v. Mastro's Rests. LLC, 952 F.3d 372, 375 (D.C. Cir. 2020) (quoting Boyd v. Kilpatrick Townsend & Stockton, 164 A.3d 72, 81 (D.C. 2017)). The existence of an express contract does not necessarily preclude the existence of additional, implied terms "inferred from the conduct of the parties in the milieu in which they dealt." Emerine v. Yancey, 680 A.2d 1380, 1383 (D.C. 1996) (quoting Vereen v. Clayborne, 623 A.2d 1190, 1193 (D.C. 1993)).[6]

[6] Contrary to CareFirst's suggestion that Plaintiffs' implied contract theory is a new argument, Plaintiffs' complaint alleges that "an implied contract was created whereby

Plaintiffs' briefing is muddy as to exactly what implied contractual duty CareFirst breached or the basis for inferring the existence of such an implied duty. Their opposition brief states that "[a]n implied term in each contract is that Defendants will use adequate measures to safeguard Plaintiffs' and members' information," citing a passage from CareFirst's corporate representative deposition in which the deponent acknowledged that CareFirst had to "put in place security safeguards to protect" PII. Opp'n at 6 (citing MSJ, Ex. C at 43:13–16). The opposition also suggests that CareFirst's security practices must be "reasonable under the circumstances" and that CareFirst failed to "act in a reasonable manner" with respect to data security. Id. Elsewhere in the opposition, Plaintiffs detail more specific security failures, for instance, a failure to train employees properly and to implement particular kinds of database monitoring, which the Court discusses in greater detail below. Id. at 6, 7–12.

Although Plaintiffs' recitation of this implied contract argument does not identify a particular history, course of dealings, or series of statements to support the existence of an implied contractual term of this sort, the Court follows the lead of other federal courts that have found an implied contractual duty to take reasonable measures to secure customer PII under similar circumstances. See In re Arby's Rest. Grp. Inc. Litig., No. 17-CV-0514-AT, 2018 WL 2128441, at *16 (N.D. Ga. Mar. 5, 2018) (citing cases). Generally, these decisions rest on the principle that when a consumer provides sensitive information to a merchant or business, such as credit card numbers (or, in this case, names, birth dates, and email addresses), "she intends to provide that data to the merchant only" and would not expect "the merchant to allow unauthorized third-parties to access that data," resulting in "an implicit agreement to safeguard

Defendants' [sic] promised to safeguard Plaintiffs' health information and Sensitive Information from being accessed, copied, and transferred by third parties." SAC ¶ 70.

the data" in order to effectuate the contract. Anderson v. Hannaford Bros. Co., 659 F.3d 151, 159 (1st Cir. 2011). As one court observed, "it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently." Castillo v. Seagate Tech., LLC, No. 16-CV-01958-RS, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016).[7]

This is not to say that every data breach will give rise to a valid claim for a breach of an implied contract. But the conduct of the parties here is instructive, particularly CareFirst's Notice of Privacy Practices, which describes how the company may "use, disclose (share or give out), collect, handle and protect our members' protected health information" and represents that the company "maintain[s] physical, electronic and procedural safeguards in accordance with federal and state standards to protect your health information." MSJ, Ex. Z at 1. Unlike the Privacy Statements in Plaintiff's insurance agreements, the Notice of Privacy Practices speaks of

[7] To be sure, not all courts have agreed. For instance, CareFirst cites Gaddy v. Long & Foster Cos., No. 21-2396, 2022 U.S. Dist. LEXIS 46657 (D.N.J. Mar. 15, 2022), which dismissed a breach of implied contract claim arising from a data breach. Looking to confidentiality agreements similar to those at issue here, Gaddy held that such provisions did not give "rise to a plausible inference that Long & Foster implicitly promised to ward against the *theft* of Plaintiffs' PII by hackers," only a duty to avoid "*intentional disclosure* of employee PII." Id. at *25–27 (emphasis in original). Such decisions buck the weight of authority, however, and CareFirst's Notice of Privacy Practices, moreover, goes beyond merely addressing intentional disclosures. MSJ, Ex. Z at 1. The Court also is not persuaded by CareFirst's reliance on Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. 2017). There, the Eighth Circuit rejected an implied contract claim because the complaint did not specify "how Scottrade failed to take 'industry leading' security measures" to protect customer PII. Id. at 718; see also Anderson v. Kimpton Hotel & Rest. Grp., LLC, No. 19-CV-01860-MMC, 2019 WL 3753308, at *5 (N.D. Cal. Aug. 8, 2019) (dismissing implied contract claim where plaintiffs did not "plead any facts to support" the "conclusory assertions" regarding a failure to take reasonable steps to protect PII). By contrast, as discussed below, Plaintiffs here have amassed at least some evidence concerning measures that CareFirst could or should have taken to reduce the risk that hackers would pilfer member data.

an obligation to take affirmative steps to "protect" member PII. In light of the Notice of Privacy Practices and the fact that Plaintiffs must provide certain PII to use CareFirst's online web portal, MSJ, Ex. C at 297, the Court agrees with the courts cited above that CareFirst made an implied promise to take reasonable steps to secure Plaintiffs' PII against threats from third-party hackers. This was a promise that would substantially overlap with, if not include, HIPAA's requirements that covered entities ensure "the confidentiality, integrity, and availability of all electronic protected health information" and protect "against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. §§ 164.306(a)(1)–(2). Whether CareFirst has breached that implied duty, however, is a closer question, to which the Court now turns.

2. Breach

CareFirst asserts that, even if it had a contractual duty to take reasonable steps to secure member PII, it did not breach that duty. MSJ at 13; Reply at 8–9. As evidence that CareFirst acted reasonably, the company points out that the Health and Human Services ("HHS") Office of Civil Rights requested information concerning the company's data security practices sometime after the breach but eventually closed its investigation without finding any HIPAA regulation violations. DSUF ¶ 26. CareFirst also points to a 2013 data security audit by KPMG, which observed that CareFirst had "created a robust security awareness program," had "enhanced physical security capabilities," and had begun implementing "a wide variety of tools and technological solutions" to safeguard PII. MSJ, Ex. O at 290. Additionally, CareFirst's expert report by data-security analyst Ronald Yearwood posits that CareFirst was compliant with its privacy policies, citing its implementation of firewalls and intrusion detection systems, its maintenance of workstation and equipment use policies, and its monitoring of access to sensitive

files and systems. MSJ, Ex. BB at 15–16; see also DSUF ¶¶ 28–32 (highlighting a laundry list of CareFirst's technological and procedural safeguards for data protection); MSJ, Ex. A (House Decl.) ¶ 23.

In response, Plaintiffs rely almost exclusively on the report of their own data-security expert, Matthew Strebe, who outlines a series of purported shortcomings in CareFirst's data security practices that, he maintains, permitted the hackers to exfiltrate Plaintiffs' PII. See Opp'n at 7–12; PSMF ¶¶ 13–32. But expert opinion alone cannot create a genuine dispute of fact. As CareFirst points out, "a party cannot avoid summary judgment when it offers an expert opinion that is speculative and provides no basis in the record for its conclusions." Martin v. Omni Hotels Mgmt. Corp., 321 F.R.D. 35, 40 (D.D.C. 2017); accord Crystal Prods., Inc. v. Doc Severinsen Orchestras, No. CIV.A. 90-932, 1994 WL 507546, at *3 (D.D.C. Sept. 10, 1992) ("Where a party opposing summary judgment relies on expert opinion to support its position, summary judgment is nevertheless appropriate if the expert's opinion has no basis other than theoretical speculations."). On that note, Strebe's report does not inspire a great deal of confidence. As discussed below, it is often difficult to gauge the validity of Strebe's conclusions about CareFirst's practices, either because he does not cite any materials to support his statements or because Plaintiffs have not included or identified the cited materials in the evidence filed with their summary judgment materials. Based on the evidence that Plaintiffs have included, however, the Court will now proceed to evaluate whether the record could support Strebe's conclusions about CareFirst's various data security deficiencies.

a. Failure to Engage a Full-Scale Incident Response Plan and Examine the Network

First, Plaintiffs assert that after learning about the spear phishing email in April 2014, CareFirst "failed to engage its full-scale incident response plan, failing to examine the network,

as well as the Security Incident and Event Monitoring ('SIEM') System, which would have revealed further indicators of an attack or compromise of Defendants' network." Opp'n at 8; PSMF ¶¶ 17–18. Although Plaintiffs cite page 24 of the Strebe report for support, the relevant pages appear to be pages 19–20 and 25–26. See MSJ, Ex. CC (Strebe Report) at 19–20, 25–26 (Page 24 focuses instead on "whitelisting" servers and security training.)

Strebe's support for these conclusions is thin, at best. At the time of the data breach, CareFirst used a product called ArcSight SIEM, a security incident event management tool that examines "large volumes of logs and data to look for patterns of abnormality." MSJ, Ex. C at 205; see also MSJ, Ex. B ¶ 39; MSJ, Ex. CC at 8 ("SIEM software collects the logs of all the devices on a network including computers, servers, networking equipment, and security equipment, and feeds them into a centralized system where they are filtered, processed, aggregated, and analyzed automatically, generating bigger-picture events and alerts which are exposed to human security operators for action, typically via graphing dashboards."). Strebe speculates that CareFirst failed to configure its SIEM system properly because, at some point, AT&T apparently notified CareFirst of some suspicious activity within its network. MSJ, Ex. CC at 20 ("When AT&T notified Care First that it had botnet participants operating inside its network, [CAREFIRST-054755] indicated that CareFirst was overrun with malware *that it did not know about* due to its deficient human monitoring of the SIEM and anti-malware logs which were not being shipped to the SIEM." (emphasis in original)). But Plaintiffs have not cited, nor can the Court find in the filed summary judgment materials, the purported supporting evidence—apparently an email, which is referred to in deposition transcripts in the record, MSJ, Ex. C at 54–75; MSJ, Ex. DD at 112–113.

From what the Court can glean about the email, however, it does not appear to support Strebe's conclusory assertions. The AT&T email was sent before the breach and had nothing to do with the type of cyberattack at issue in this case. MSJ, Ex. C at 59 ("Q. Okay. And let's be clear. This breach has nothing to do with a DDOS attack, correct? . . . A. Correct."). Moreover, as CareFirst's 30(b)(6) deponent testified, and as Strebe himself acknowledged, CareFirst actually had discovered and addressed the suspicious activity discussed in the AT&T email *before* the email was sent. Id. at 60, 306; MSJ, Ex. DD at 91. Thus, setting aside the inapposite AT&T email, Strebe's assertion that CareFirst failed to configure SIEM properly is not supported by any citation. See MSJ, Ex. CC at 20 ("Routine monitoring of numerous system logs was obviously not occurring, and events were recorded that would have flagged observant administrators to ongoing threat actor activity."). Nor does Strebe provide citations for statements like "it never seems to have occurred to anyone that they should engage their full-scale incident response plan and examine the network and the SIEM." Id. at 26.

Additionally, Strebe contends that CareFirst's ArcSight SIEM system "was deficient." Id. at 19. That conclusion, it seems, is premised on the reasoning that CareFirst, at some point, replaced one SIEM system (ArcSight) with another one (QRadar), "because it could integrate Sophos [antivirus] logs." Id. ArcSight, Strebe explains, "was also capable of ingesting Sophos [antivirus] logs at the time," and so Strebe speculates that CareFirst's justification for replacing ArcSight with QRadar "indicates that nobody at CareFirst knew how to use or configure it to do so." Id. In addition to the fact that this theory is fairly speculative—divining CareFirst's improper use of antivirus technology from its alleged justification for changing to a different SIEM system—the Court again cannot find in the evidentiary record submitted with the summary judgment briefing any document supporting Strebe's statement that CareFirst switched

to QRadar for reasons that demonstrated an unfamiliarity with the SIEM system. What evidence the Court has been able to locate rather suggests that CareFirst switched to QRadar because of its "heavy investment in IBM at the time" and its judgment that QRadar was "a better platform to move to [because it] could serve [CareFirst's] needs better and perform a better job." MSJ, Ex. C at 229–30.

Strebe also asserts that CareFirst "failed to change administrative credentials across the board," but his citation to a Bates-stamped page numbered CAREFIRST-000223 is followed by a parenthetical stating, "check this cite for applicability." MSJ, Ex. CC at 26. On its own, the Court has located some evidence that CareFirst did not require "all users and administrators to reset their passwords" after the breach. See MSJ, Ex. C at 277. Elsewhere, however, CareFirst's 30(b)(6) deponent states that some number of users did have to change passwords, id. at 215, a statement consistent with the Mandiant report's finding that CareFirst performed a targeted password reset for users who had downloaded the malicious software, MSJ, Ex. Q at 3–4. Even assuming that CareFirst did not require the relevant employees to change their credentials and that such a requirement would have stopped the cyberattack, Plaintiffs nowhere explain why CareFirst's failure to change administrator credentials was unreasonable under the circumstances, given that CareFirst apparently did not know its employee may have exposed his administrator credentials when he clicked the malware link. See MSJ, Ex. A ¶ 15; MSJ, Ex. C at 257, 147 (Doyle "testified internally that he did not" use administrator credentials when he clicked the link).

Accordingly, the Court concludes that Strebe's assertions regarding CareFirst's initial response to the cyberattack and its use of SIEM software are speculative, unsupported by record evidence, and therefore do not create a genuine dispute of material fact.

b. Failure to Properly Train Employees

Plaintiffs next maintain that CareFirst failed to train its employees adequately on recognizing spear phishing attempts and on properly using privileged accounts. Opp'n at 8–10; PSMF ¶¶ 19–24; MSJ, Ex. CC at 24–25. On this point as well, Strebe's report is decidedly conjectural. Strebe states that among his company's customers who do not use spear phishing resistance training, 25–40% of users fail to identify phishing messages, versus 1–3% for those customers who have received professional anti-spear phishing training. MSJ, Ex. CC at 24. Strebe then states that, according to the Mandiant report, the spear phishing cyberattack on CareFirst "was engaged against five users in the environment, two of whom clicked on the link," comprising a 40% failure rate. Id. From this, Strebe deduces that CareFirst "obviously lacked spear-phishing resistance training for its end users." Id.

There are multiple problems with this conclusion. For starters, Strebe's numbers are wrong. The Mandiant report states that the spear phishing campaign targeted 48 CareFirst employees, six of whom clicked on the malicious link, and five of whom (a subset of the six) downloaded and ran malicious software. MSJ, Ex. Q at 3; see also MSJ, Ex. C at 135–39.[8] Six out of 48 employees would amount to a 12.5% failure rate, not Strebe's hypothetical 40% failure rate. Even if he were right about the underlying figures, Strebe acknowledges that "there is a small-numbers sampling problem in a five-user sample." MSJ, Ex. CC at 24. Moreover, the report in no way addresses CareFirst's evidence that it *does* train its employees on data security. See DSUF ¶ 30. Further, whether or not CareFirst's employees could recognize a spear phishing

[8] The Court cannot tell how Strebe procured his figures. Plaintiffs' statement of undisputed material facts makes the same error—stating that two of five targeted employees downloaded the malicious software—but they cite the page of the Mandiant report that contains the opposing figures discussed above. PSMF ¶ 1.

email is irrelevant to Plaintiffs' theory of how the cyberattack succeeded, which is that Doyle, knowing full well that the email was a spear phishing attempt, nevertheless improperly went rogue to investigate the attack and unwittingly gave the hackers access to his administrator credentials. MSJ, Ex. CC at 25 ("Wesley Doyle's naïve attempt at investigation opened the backdoor . . . ."); PSMF ¶ 22 ("Mr. Doyle investigated the infected email on his own recognizance . . . ."); MSJ, Ex. C at 143–44.

Apart from this conjecture about phishing failure rates, Strebe and Plaintiffs assert that, with proper training, Doyle would not have used his administrator privilege account when he clicked the malware. Opp'n at 9. But it is not clear from the record that Doyle was using his administrator account when he clicked on the malware link, as the hackers could have accessed administrator credentials stored in his machine's cache even if he was using his non-privileged user account. MSJ, Ex. C at 145–73. And even if Doyle happened to access the malware via his administrator account, Strebe's report states that CareFirst *did* employ the best practice of requiring "admin users to use low privileged accounts for their routine work." MSJ, Ex. CC at 24. For further support that reasonable steps could have avoided Doyle's error, Plaintiffs cite the following exchange from the deposition of CareFirst's data security expert:

> Q: And would you agree that with proper administrative safeguards, Mr. Doyle would have had the knowledge not to click on an identified spear phishing malware link? . . .
>
> THE WITNESS: So I don't know what the history of safeguards would have – and I mean if we're thinking administrative safeguards as far as additional training, perhaps that's possible, that with additional training he may . . . have had a different perspective. I don't know . . . . I can't say that he didn't receive training . . . regarding phishing or . . . other topics.

Opp'n, Ex. C at 137. This exchange is no smoking gun. Rather, it is entirely non-committal and not based on any concrete facts about Doyle's training or what additional training might have

changed his behavior.[9] Plaintiffs thus have not created a genuine dispute of material fact as to whether CareFirst employees were properly trained against spear phishing attacks.

c. Failure to Implement Network Segmentation and Search for Lateral Movement

Next, Plaintiffs contend that CareFirst failed to implement proper segmentation—essentially the placement of digital borders between various internal computer systems—and failed to monitor traffic flowing between such segments to prevent hackers from engaging in "lateral movement" between computer systems. PSMF ¶¶ 25–26; MSJ, Ex. CC at 18–19. Unlike Plaintiffs' previous theories, the contention that CareFirst failed to monitor potential lateral movement sufficiently in the wake of the initial spear phishing incident creates a genuine dispute as to the element of breach.

Strebe's report acknowledges that "CareFirst has stated that it implements network segmentation." MSJ, Ex. CC at 19. Based on the fact that attackers nevertheless moved through the network without detection, however, Strebe asserts that CareFirst did not adequately monitor the metaphorical "borders" between digital segments. Id. Once again, however, Strebe cites no evidence to support this contention, and the record, to the contrary, suggests that CareFirst did in fact monitor for such traffic as a general matter. See MSJ, Ex. C at 184–85 (stating that CareFirst looked for lateral movement in April 2014 and at other times); id. at 213 ("We monitored for activity from the suspect segment and did not see any indication of traffic coming

[9] Strebe repeatedly suggests that CareFirst must have known that Doyle used his administrator credentials when he clicked on the link, relying on the notion that CareFirst "reprimanded" Doyle for doing so. MSJ, Ex. CC at 24–25. Again, the record does not establish that Doyle used his administrator credential when he clicked the link. And the statement lacks support in any case, with Strebe adding the parenthetical "[cite reprimand]" after making this assertion. Id. at 24. CareFirst's 30(b)(6) deponent, moreover, made clear that Doyle was reprimanded for accessing the spear phishing message, *not* because CareFirst believed he used a privileged account in doing so. See MSJ, Ex. C at 166–67.

from there."); id. at 195–201 (explaining that there were "blocks" for "the known indicators of compromise into our firewalls, and so they would have shown up as firewall blocks in the logs"); id. at 203 ("The sensors that we had at the time were cross-network segment sensors. So the degree that the communication was externally to something in another segment of our network that had a sensor between the two, then we could have seen that traffic."); id. at 204 ("As part of our standard monitoring, we capture that traffic."); id. at 207 (noting that the "SIEM platform . . . has correlation rules that look for abnormalities" to monitor lateral movement).

Despite the dearth of evidence in Strebe's report to support his conclusion that CareFirst did not properly segment or monitor the segmentation of its computer systems, Plaintiffs have identified one document from which a reasonable jury might conclude otherwise: an email in which CareFirst's chief security officer, Don Horn, responding to another IT official's request for information about the company's conduct after the phishing incident, stated that the IT team "did not look for lateral movement" after the phishing incident. Opp'n, Ex. L at 6–8. But even this evidence is mixed. Horn's email proceeds to state that the IT team "jumped on the incident quickly and had no reason to suspect that the attacker moved even faster," adding that company IT "monitored for activity from the suspect segment . . . and did not see any indication of traffic coming from there," language which sounds similar to looking for lateral movement. Id. at 6. According to CareFirst's corporate deponent, Horn's description was incorrect and the company "had documentation from a member of his staff indicating that some steps were taken to look for . . . lateral movement." MSJ, Ex. C at 209; see also id. at 205–13. That "documentation" appears to be another email in the chain with Horn, in which another CareFirst cybersecurity specialist described monitoring of traffic to and from the workstations and domain associated with the phishing attack. Opp'n, Ex. L at 4–5. But even so, that cybersecurity specialist

conceded that, "[i]n retrospect," CareFirst's monitoring should have been more comprehensive and that the company "should have had a protocol or a process for monitoring *all* remote access involving the credentials associated with these users" "across the enterprise," which would have provided "some indication that the perimeter had been breached." Id. at 5.

Reading this evidence in the light most favorable to Plaintiffs, these emails, although their conclusions are disputed by CareFirst, create a genuine question about whether CareFirst searched adequately for lateral movement in the immediate aftermath of the spear phishing attack.

d. Failure to Implement Database Access Monitoring

Last, Plaintiffs maintain that CareFirst failed to implement "Database Access Monitoring," or "DAM," a practice of logging database queries (such as commands to insert, update, delete, or alter data) and setting alerts for the use of specific commands (such as mass deletions of data) which might signal nefarious activity. Opp'n at 11; PSMF ¶¶ 27–30; MSJ, Ex. CC at 20–21. Here, again, Plaintiffs' contention has modest support in the record and creates a genuine dispute of material fact as to breach.

The Strebe report cites an internal CareFirst document which appears to post-date the 2014 phishing attack and which, according to CareFirst, was prepared to obtain internal approval of a plan to implement DAM. See Opp'n, Ex. L at 2; Reply at 9 n.5. At one point, the document states that failure to implement DAM "leaves CareFirst databases vulnerable to inappropriate access to protected information, leading to non-compliance with HIPAA regulations that can lead to criminal penalties and fines, and an inability to respond to the audit findings." Id. Pointing to this statement, Strebe opines that properly configured DAM would have more quickly detected the unauthorized access to CareFirst's network resulting from the 2014 phishing

attack. MSJ, Ex. CC at 21. CareFirst addresses DAM only in a footnote in its reply brief and does not deny that it had not implemented DAM as of 2014. See Reply at 9 n.5. Rather, CareFirst cites a portion of Strebe's deposition testimony, in which CareFirst's lawyer pointed out that the use of DAM did not stop similar hacks of Anthem and Premera, which had implemented DAM. Reply at 9 n.5; MSJ, Ex. DD at 125. Strebe's full deposition testimony, however, goes on to opine that, in the Anthem and Premera cases, DAM was not "properly configured to alert" users to suspicious activity and that, based on his work in those cases, DAM "did provide numerous indicators of attack prior to the exfiltration" of data. Id. at 125–26.

CareFirst also argues that "the DAM tool," even if implemented, "would not have been able to detect lateral movement," Reply at 9 n.5, but that observation appears to be beside the point. Although detecting suspicious lateral movement was one way in which CareFirst might have caught the hackers, Strebe contends that DAM could have detected them in different ways, for example, by alerting CareFirst IT to the use of "high-threat queries" in the company's databases, such as those deleting or moving large amounts of data. MSJ, Ex. DD at 123. The Court therefore concludes that Plaintiffs have established a genuine factual question as to whether the implementation of DAM was the sort of reasonable data-security measure that could have abated the 2014 cyberattack.

e. Conclusion

In sum, although many of the purported security flaws on which they rely lack factual foundation, Plaintiffs have pointed to at least some evidence to support the conclusion that CareFirst failed to search for lateral movement after the spear phishing incident and failed to implement DAM. Plaintiffs do not provide much legal argument, however, as to the more difficult question: whether a jury could find that either or both of these failures constituted a

breach of CareFirst's implied contractual duty to take reasonable steps to safeguard member PII and to comply with HIPAA's data-security standards, to the extent they also require covered entities to take reasonable precautions to safeguard protected data. Nevertheless, the Court concludes that a jury must ultimately answer that question.

"While in some rare cases where there is no controversy over the facts, the issue of whether a party to a contract has breached a contractual provision is also a question of law, generally whether there was a breach of the terms of a contract is a question of fact." 23 Williston on Contracts § 63:15 (4th ed.) (footnotes omitted). Put another way, "[w]ith respect to assertions that a contract has been breached, '[t]he determination whether a material breach has occurred is generally a question of fact'" but may reduce to a question of law only if there is but "one reasonable conclusion." America v. Preston, 468 F. Supp. 2d 118, 122 (D.D.C. 2006) (second alteration in original) (quoting 23 Williston on Contracts § 63:3 (4th ed.)). Particularly with respect to breaches that turn on the reasonableness of the breaching party's actions, however, whether the defendant's conduct constitutes a breach of a contract is usually a jury question. See, e.g., 17B C.J.S. Contracts § 1041 ("Questions of the reasonableness of behavior or performance under a contract expressly or impliedly calling for reasonable effort or behavior are generally questions of fact as under a provision for commercially reasonable efforts. . . . The question becomes one of law in the absence of an issue of material fact when only one inference can be drawn from the evidence or when reasonable minds could not differ or could come to only one conclusion." (footnotes omitted)); VKGS, LLC v. Planet Bingo, LLC, 962 N.W.2d 909, 920 (Neb. 2021) ("Typically, the question of whether reasonable measures were taken to keep information confidential is an issue for a jury."); Informed Physician Servs., Inc. v. Blue Cross & Blue Shield of Md., Inc., 711 A.2d 1330, 1342 (Md. 1998) ("[W]hat will constitute reasonable

efforts under a contract expressly or impliedly calling for them is largely a question of fact in each particular case and entails a showing by the party required to make them of 'activity reasonably calculated to obtain the approval by action or expenditure not disproportionate in the circumstances.'" (quoting Allview Acres v. Howard, 182 A.2d 793, 796 (Md. 1962))).

Here, whether Plaintiffs' theory of breach turns on HIPAA's regulatory standards or on what data security practices are reasonable in the abstract, either basis for liability is essentially premised on the reasonableness of CareFirst's data security measures. Although Plaintiffs do not cite any provisions of HIPAA that they allege were violated, CareFirst concedes that the "HIPAA Security Rule contemplates a flexible approach, as '[c]overed entities . . . may use any security measures that allow the covered entity . . . to *reasonably* and *appropriately* implement the standards and implementation specifications as specified in this subpart.'" MSJ at 13 (emphasis added) (quoting 45 C.F.R. § 164.306(b)(1)). Although HIPAA regulations also set forth more specific requirements, the lodestar in the analysis is reasonableness.

To be sure, there is also evidence in the record—a great deal of it—that supports CareFirst's contention that it took adequate measures to protect Plaintiffs' PII. Among other things, CareFirst has pointed to audits by KPMG showing a high degree of compliance with HIPAA privacy and security standards, has produced an expert report further describing the company's data security efforts, and has included in its filings a multitude of documents evidencing the existence of internal security compliance policies. See MSJ, Ex. BB (Yearwood report); MSJ, Ex. O at 286–305 (2013 KPMG audit); id. at 306–44 (2014 KPMG audit); id. at 290 (stating that CareFirst "has created a robust security awareness program" and has implemented "a wide variety of tools and technological solutions to assist in safeguarding" PII); id. at 291 (stating that CareFirst "complies to some level with 99% of the CMS audit protocols");

id. at 1218–1300 (information security compliance manual). But see MSJ, Ex. O at 292–95 (pointing out areas for improvement, including lacking "a complete understanding of where all [Electronic Personal Health Information ('ePHI')] is housed, accessed, transmitted, or managed").[10]

On the other side of the balance, moreover, neither Strebe's expert report nor his defense of that report in his deposition inspires much confidence. In addition to the missing citations and speculation in his report, Strebe appeared to walk back some of his written opinions in his deposition. See MSJ, Ex. DD at 115 (acknowledging that Strebe "would give [CareFirst] a pass for not being able to detect" certain forms of lateral movement "because a lot of that technology's newer"); id. at 103 (considering whether he needs to revise report's statement that certain security tools were "common" in 2014); id. at 105–06 (acknowledging that statement that the hacker could not have gotten administrator credentials had CareFirst better monitored those credentials "is a little bit incorrect" and "a little bit erroneous"); id. at 112 ("well, okay, I don't want to be that assertive"). At other times, Strebe showed a lack of awareness of some important facts in the record. See id. at 117 (stating that he was not aware that it took Mandiant 70 scans of CareFirst's systems to discover evidence of the breach, after writing in his report that the breach was "easily found by Mandiant").

[10] As noted previously, CareFirst also relies on the decision of HHS's Office of Civil Rights to close its investigation into the company's data breach without finding any HIPAA violations. MSJ at 21. HHS's closure letter, however, at most states that, as of the investigation's closure in 2021, CareFirst had "taken numerous steps to enhance its security posture by employing additional policies and procedures to continue reducing risk to its ePHI environment." MSJ, Ex. P at 5. The fact that HHS closed its investigation does not, without more, prove that CareFirst had taken reasonable steps to protect customer PII as of 2014 and 2015.

At this stage, however, the Court cannot make credibility determinations or weigh the evidence; those tasks must be left to a jury. Barnett, 715 F.3d at 358. Whatever the Court's view of who has the stronger case, Plaintiffs have pointed to more than "a scintilla of evidence" from which a reasonable jury could conclude CareFirst breached its promise to take certain reasonable steps to safeguard their PII. Chen v. Bell-Smith, 768 F. Supp. 2d 121, 133 (D.D.C. 2011) (quoting Anderson, 477 U.S. at 252).

3. Causation

In its reply brief, CareFirst also contends that summary judgment is warranted because Plaintiffs have not established causation. Reply at 9–10. Because CareFirst did not raise this argument in its opening brief, and thus Plaintiffs had no opportunity to address it, CareFirst's objection to causation is waived. Shands Jacksonville Med. Ctr. v. Burwell, 139 F. Supp. 3d 240, 260 n.7 (D.D.C. 2015) (citing New York v. EPA, 413 F.3d 3, 20 (D.C. Cir. 2005)).

Even if the argument were not waived, the Court does not find it persuasive. CareFirst maintains that the cause of the breach was Doyle's clicking on the malware link with his administrator credentials and that there "is no evidence in the record suggesting any other cause for how the hackers gained access." Reply at 9–10. That Doyle's initial actions may have triggered the cyberattack may be true, but it is irrelevant to legal causation. Plaintiffs' theory is that CareFirst's database security deficiencies led to failures to detect and thwart the hackers *after* they were given access, which is what Plaintiffs maintain enabled the exfiltration of their PII. That Doyle was solely responsible for permitting the initial access is immaterial to that theory of breach.

4. Damages

Finally, CareFirst renews its previous argument that Plaintiffs have not shown actual damages. MSJ at 15–18; Reply at 10–12. This question has already been litigated in this case. In Attias III, the Court granted Plaintiffs' motion for reconsideration of the prior decision to dismiss Plaintiffs' contract claim and permitted that claim to proceed on the theory that a prevailing party might be eligible for nominal damages, even if actual monetary damages cannot be proved and even if Plaintiffs' costs associated with mitigating the risk of identity theft do not constitute actual damages. 518 F. Supp. 3d at 48, 52.

CareFirst acknowledges that ruling, but insists that dismissal is warranted nonetheless because any nominal damages available here are *de minimis*. MSJ at 17. For this argument, CareFirst relies on Henson v. Prue, 810 A.2d 912 (D.C. 2002). There, the D.C. Court of Appeals upheld a trial court's verdict that the plaintiff's eviction was unlawful, which included an award of an injunction but no damages. Id. at 916. The court stated that although it could theoretically remand the case with instructions to award nominal damages, "[s]uch a remand would . . . be symbolic only" and the failure of the trial court to award nominal damages was "not a ground for reversal." Id. (quoting Lee v. Dunbar, 37 A.2d 178, 180 (D.C. 1944)); id. ("[A] judgment for plaintiff will not be reversed on appeal for a failure to award nominal damages, even though plaintiff is entitled to recover nominal damages as a matter of law." (quoting Kraisinger v. Liggett, 592 P.2d 477, 480 (Kan. 1979))). Henson, therefore, stands only for the proposition that a failure to award nominal damages is not a ground for reversal and remand on appeal; it does not hold that Plaintiffs' case here should be dismissed simply because nominal damages are, as a rule, *de minimis*.

Plaintiffs also contend that, in addition to nominal damages, (1) the Tringlers have shown possible entitlement to actual damages stemming from tax fraud they purportedly suffered after the CareFirst breach and (2) mitigation expenses should qualify as actual damages. Opp'n at 23–24. Because, as Plaintiffs do not dispute, tax fraud would only be possible through the use of the Tinglers' Social Security or tax identification numbers, Plaintiffs suggest there is a genuine dispute about whether the hackers here accessed such information, as opposed to only Plaintiffs' names, dates of birth, web portal usernames/email addresses, and CareFirst subscriber identification numbers. PSMF ¶ 6–7. But there is no evidentiary support for this conclusion. The only evidence Plaintiffs cite is CareFirst's breach notification letter sent to affected members in 2015, which stated that, based on the Mandiant investigation, it "appears that attackers had access to your name, subscriber ID, email address and date of birth as well as the user name that you setup [sic] as part of your registration to use the site." Opp'n, Ex. I at 1. Plaintiffs emphasize that the use of the word "appears" leaves room for doubt that more information might have been breached. PSMF ¶ 6. But that interpretation of the letter is belied by the letter itself, which goes on to explain that "the attackers did not gain access to your medical information, claims information, Social Security number, credit card, financial information or any other information about you." Opp'n, Ex. I at 1. To boot, the suggestion that the hackers accessed Social Security or other taxpayer numbers is rebutted by other uncontradicted evidence, including the Mandiant report, MSJ, Ex. Q at 4 (noting that CareFirst member data did not include Social Security or taxpayer ID numbers), and CareFirst's 30(b)(6) deponent's testimony, MSJ, Ex. C at 225–26.

Plaintiffs next assert that, "even assuming that the hacker(s) did not access the Tringer's [sic] Social Security numbers"—as the undisputed record shows—"the information obtained in

the breach was entirely sufficient to execute a successful identity theft against not just the Tringlers, but all Plaintiffs." Opp'n at 23. Plaintiffs raise two arguments to support this claim.

First, Plaintiffs posit that the D.C. Circuit, in this case, already concluded that the information involved in this breach could be combined to commit identity theft and fraud "even if the compromised information did not include plaintiffs' social security numbers." Id. The Circuit did not so hold. What the Circuit said, and what this Court restated in its opinion granting partial reconsideration, was that the *complaint alleged* that CareFirst stored PII—including credit card and Social Security numbers—and that, even absent a breach of Social Security numbers, Plaintiffs faced a risk of some forms of medical identity fraud sufficient to plead standing. See Attias I, 865 F.3d at 628; Attias III, 518 F. Supp. 3d at 47–48. Neither the Circuit nor this Court ruled that the evidence in fact *supported* such an allegation in this case. In light of the now developed record, which shows that the information required to commit the Tringlers' tax fraud was not a part of the CareFirst breach, the assertion that the breach caused the Tringler's purported experience with tax fraud is simply not plausible.[11]

Second, Plaintiffs point to a statement in their damages expert report, by Daniel J. Korczyk, that "it does not take much stolen information to put a person's finances at risk . . . [one's] name and address are enough information to serve as a gateway to steal [someone's]

[11] The only other evidence Plaintiffs cite regarding the Tringlers is Mrs. Tringler's deposition testimony, in which she affirmatively answered counsel's question, "Did the Maryland Comptroller connect your tax return fraud to the CareFirst breach?" MSJ, Ex. H at 39. Setting aside the probability that this statement is inadmissible hearsay, this response to a leading question from Plaintiffs' counsel cannot create a genuine question for a jury in light of the overwhelming evidence that Plaintiffs' Social Security and tax ID numbers were simply not part of the CareFirst breach. Indeed, the more plausible interpretation of Mrs. Tringler's statement is that an official with the Maryland Comptroller indicated he or she "had seen the letter" sent by CareFirst, MSJ, Ex. G at 48 (Curt Tringler deposition), a fact that would "connect" the tax fraud to the breach, but not in any meaningful way.

identity." Opp'n at 23–24.[12] Plaintiffs' suggestion, it seems, is that the theft of the information here—limited to member names, subscriber ID numbers, date of birth, and email addresses—could have opened the door to hackers to procure member Social Security numbers through different avenues, which in turn could have enabled someone to obtain the Tringlers' tax refund. Aside from Korczyk's statement, Plaintiffs cite no evidence that such a conjectural series of events actually happened in this case. Such "[m]ere speculation is not enough to survive summary judgment." Atanus v. Sebelius, 652 F. Supp. 2d 4, 10 (D.D.C. 2009); see also Byrd v. EPA, 174 F.3d 239, 248 n.8 (D.C. Cir. 1999) ("It is well settled that [c]onclusory allegations unsupported by factual data will not create a triable issue of fact." (alteration in original) (quoting Exxon Corp. v. FTC, 663 F.2d 120, 126–27 (D.C. Cir. 1980))).

Finally, with respect to whether their expenditures on mitigation measures in response to the data breach may constitute actual damages, Plaintiffs attempt to distinguish this case from Randolph v. ING Life Insurance and Annuity Co., 973 A.2d 702 (D.C. 2009), where the D.C. Court of Appeals held that costs "incurred to undertake credit monitoring or other security measures to guard against possible misuse of" breached data are "not the result of any present injury, but rather the [result of] the anticipation of future injury that has not materialized," id. at 708 (citation omitted). Plaintiffs suggest this case is not governed by Randolph, despite the Court's previous conclusion, because Randolph noted in a footnote that "there is no evidence that the burglary" resulting in the theft of an ING employee's laptop containing plaintiffs' data "was undertaken for the specific purpose of obtaining the information on the laptop." Id. at 704

[12] Plaintiffs cite Exhibit A to their opposition but did not attach the correct pages of the Korczyk report. The Court was only able to review the correct pages because they were also submitted as an exhibit to Plaintiffs' motion for class certification. See Mot. for Class Cert, Ex. 7 at 22, ECF No. 89-7.

n.2. That footnote, however, had no bearing on the court's conclusion that mitigation expenses did not constitute actual harm. This argument therefore fails.

* * *

For the foregoing reasons, although their recovery is almost certainly limited to nominal damages, Plaintiffs have created a genuine dispute of material fact as to their breach of contract claim. The Court, accordingly, denies CareFirst's motion for summary judgment as to that claim, with one caveat: CareFirst argued in its motion that two of the named defendants—CareFirst, Inc. and Group Hospitalization and Medical Services, Inc.—did not have any contractual relationship with any of the named Plaintiffs. MSJ at 9 n.2; MSJ, Ex. B ¶¶ 3, 5, 17, 21, 24, 27, 29. Rather, only CareFirst BlueChoice, Inc. and CareFirst of Maryland, two subsidiaries of CareFirst, Inc. and Group Hospitalization and Medical Services, Inc., had contractual relationships with Plaintiffs. MSJ, Ex. B ¶¶ 15, 19, 22, 26; see also DSUF ¶¶ 9–25. Because Plaintiffs did not dispute this argument, the Court concludes that it is conceded. Mulhern v. Gates, 525 F. Supp. 2d 174, 185 n.15 (D.D.C. 2007) ("On a motion for summary judgment, the Court may assume that the non-moving party has conceded the moving party's statement of facts unless the non-moving party specifically controverts the moving party's statement."). The Court therefore grants CareFirst's motion for summary judgment on Plaintiffs' breach of contract claim as to Defendants CareFirst, Inc. and Group Hospitalization and Medical Services, Inc. only.

B. Maryland Consumer Protection Act

The Court next addresses CareFirst's contention that summary judgment is warranted on Plaintiffs' MCPA claim. Plaintiffs advance two theories for CareFirst's alleged violation of the MCPA: first, that CareFirst's Notice of Privacy Practices misrepresented that CareFirst

maintained data-security safeguards "in accordance with federal and state standards," and second, that CareFirst's investigation and notification of the data breach violated the Maryland Personal Information Protection Act ("MPIPA"), a violation of which would also constitute an MCPA violation. Neither theory can be sustained. As to the first, Plaintiffs have failed to adduce evidence that they were even aware of, let alone that they relied on, statements in the Notice of Privacy Practices. And as to the second, the data breach at issue in this case does not fall within the scope of MPIPA.

1. Misrepresentation Theory

"In a private action under the MCPA, a consumer must establish '(1) an unfair or deceptive practice . . . that is (2) relied upon, and (3) causes them actual injury.'" In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 341 F.R.D. 128, 159 (D. Md. 2022) (quoting Bey v. Shapiro Brown & Alt, LLP, 997 F. Supp. 2d 310, 319 (D. Md. 2014)). Among the unfair or deceptive practices that can support an MCPA claim are making false or misleading statements that have the capacity, tendency, or effect of deceiving or misleading consumers; representing that consumer services have a characteristic which they do not have; and failing to state a material fact if the failure deceives or tends to deceive. Md. Comm. Code § 13-301(1)–(3). If relying on a misrepresentation theory, consumers "must prove that they relied on the misrepresentation in question to prevail on a damages action under the MCPA." Bank of Am., N.A. v. Jill P. Mitchell Living Tr., 822 F. Supp. 2d 505, 532 (D. Md. 2011); accord Akins v. Fair Acquisitions, LLC, No. 1:20-cv-816 (RDA/MSN), 2021 WL 1239221, at *5 (E.D. Va. Mar. 26, 2021) ("[A] consumer bringing a claim under the [MCPA] must allege he relied on" the alleged misrepresentation." (citing Lloyd v. Gen. Motors Corp., 916 A.2d 257, 277 (Md. 2007))). "A consumer relies on a misrepresentation when the misrepresentation substantially induces the

consumer's choice." Bank of Am., 822 F. Supp. 2d at 532. "The requirement of reliance flows from the MCPA's prescription that the party's 'injury or loss' be 'the result of' the prohibited practice . . . ." Peete-Bey v. Educ. Credit Mgmt. Corp., 131 F. Supp. 3d 422, 432 (D. Md. 2015) (quoting Bank of Am., 822 F. Supp. 2d at 534).

Plaintiffs maintain that CareFirst's Notice of Privacy Practices constitutes a material misrepresentation under the MCPA. Opp'n at 16–17. In relevant part, the Notice of Privacy Practices, which is made available to CareFirst members at some point near the time of enrollment, states:

> We maintain physical, electronic and procedural safeguards in accordance with federal and state standards to protect your health information. All of our associates receive training on these standards at the time they are hired and thereafter receive annual refresher training. Access to your protected health information is restricted to appropriate business purposes and requires pass codes to access our computer systems and badges to access our facilities. Associates who violate our standards are subject to disciplinary standards.
>
> MSJ, Ex. Z at 1.

At the outset, it is questionable whether the Notice of Privacy Practices contains a misrepresentation at all. Whether the potential data security shortcomings discussed above constitute a viable misrepresentation under the MCPA depends on what a reasonable consumer would understand the Notice to represent. Sager v. Housing Com'n of Anne Arundel Cnty., 855 F. Supp. 2d 524, 558 (D. Md. 2012) ("In Maryland, whether a statement is 'misleading' is judged from the point of view of a reasonable, but unsophisticated consumer." (citing Luskin's, Inc. v. Consumer Prot. Div., 726 A.2d 702, 712 (Md. 1999)). Plaintiffs do not argue that the Notice misrepresented that CareFirst employees receive training on data privacy, that access to PII is restricted, or that employees who violate the company's standards are subject to discipline. Rather, citing the evidence discussed above and pointing to the first sentence of the Notice,

Plaintiffs contend that CareFirst misrepresented that it maintains procedural safeguards "in accordance with" federal and state law. Opp'n at 16–17. But that sentence can be read in multiple ways. On the one hand, it can be read to say that CareFirst maintains safeguards to protect health information, *as is required by* federal and state law. On the other, the Notice can be read to say that CareFirst maintains safeguards to protect health information *and that those safeguards satisfy* the federal and state standards. If the former interpretation governs, then CareFirst made no misrepresentation at all. The company did, indeed, maintain a host of physical, electronic, and procedural safeguards required by federal law to protect member data, as the 2013 KPMG audit confirms. If the latter interpretation governs, then whether there was a misrepresentation would turn on whether CareFirst actually satisfied HIPAA's standards, a question that is subject to reasonable disagreement.

The Court need not resolve how a reasonable consumer would interpret the Notice, however, because Plaintiffs have not demonstrated a genuine dispute of material fact as to reliance. As CareFirst points out, there is no evidence in the record that any of the Maryland Plaintiffs—Curt and Connie Tringler and Lisa Crider—relied on (or, indeed, even read) the Notice of Privacy Practices when they obtained insurance from CareFirst. MSJ at 25. When asked at her deposition why CareFirst was her healthcare insurance provider, Connie Tringler stated that "[i]t was through my husband's work [as an employee of Allegany County, Maryland] that we received this insurance," as CareFirst "was the health insurance provider for the County's employees at the time." MSJ, Ex. H at 15–16. In his deposition, Curt Tringler confirmed that he had CareFirst insurance because, as far as he knew, it "was the presumptive healthcare insurance provider for those employees who worked for Allegany County" during his employment. MSJ, Ex. G at 15–16. Lisa Crider similarly testified that the law firm where she

worked usually offered two health insurance plans—CareFirst and another plan—but that "almost all my life I've had BlueCross BlueShield CareFirst," suggesting she chose CareFirst because of its name recognition or her familiarity with the company. MSJ, Ex. J at 16. None of these depositions discusses any reliance on the Notice of Privacy Practices. Rather, the only evidence in the record going to Plaintiffs' reasons for choosing CareFirst suggests that they selected the carrier either because it was the insurance offered through their employment or because of their pre-existing relationship with the brand.[13]

Plaintiffs' two arguments in response are not persuasive. First, Plaintiffs assert that CareFirst "accompanied" the "option to enroll in CareFirst's online portal" with "specific promises and representations" regarding data security, and thus suggest that all Plaintiffs relied on the representations in the Notice at least when enrolling in the company's online portal, even if they did not do so when selecting CareFirst insurance. Opp'n at 17. Plaintiffs cite no evidence in the record to establish that they were prompted to review the Notice (or any other privacy statements) upon signing up for CareFirst's online portal, nor can the Court find such evidence. This bare assertion in Plaintiffs' briefing is insufficient to avoid summary judgment.

Second, Plaintiffs maintain that "[w]hether a misrepresentation substantially induces a consumer's choice is ordinarily a question for fact for the trier of fact," Opp'n at 21 (quoting Bank of Am., 822 F. Supp. 2d at 532), and that whether a consumer relied on a misrepresentation is an objective, not subjective, inquiry, meaning that the Court may presume reliance based on

[13] CareFirst also maintains that Plaintiffs cannot show reliance because members "do not even receive the Notice of Privacy Practices until after enrollment." MSJ at 25. The Court is not convinced by this argument, as CareFirst's 30(b)(6) deponent stated that the Notice is provided "at enrollment," MSJ, Ex. C at 289, which could mean just before or at the same time as the enrollment decision. In any event, when the Notice is made available to Plaintiffs is irrelevant absent any evidence that they reviewed it or considered it in their health insurance decisions.

the objective materiality of the alleged misrepresentation, Opp'n at 22. Plaintiffs raised a similar argument in their motion for class certification, citing cases that have presumed classwide reliance under the MCPA. For the reasons stated in the memorandum opinion denying class certification (without prejudice), ECF No. 100, the Court remains skeptical that classwide reliance can be presumed in this case. But, in any event, even the case on which Plaintiffs rely for this theory explains that "one must at least know whether a plaintiff was 'exposed' to the allegedly deceptive conduct even if one does not need to know whether he or she relied upon the conduct." In re Marriott Int'l, 341 F.R.D. at 158–59 (discussing New York law, but then applying that analysis to the MCPA). Here, Plaintiffs cite no evidence that they were even aware of the Notice of Privacy Practices, let alone that it influenced their decisions to obtain CareFirst insurance or to enroll in the online portal.

To be sure, Plaintiffs need not show that the alleged misrepresentation in the Notice was the but-for cause of their decision to choose CareFirst insurance. Bank of Am., 822 F. Supp. 2d at 532 (citing Nails v. S & R, Inc., 639 A.2d 660, 669–70 (Md. 1994)). But even if materiality "can be presumed from the nature of the practice" on an objective basis, the reason for that presumption is "the probability that the deceptive practice affected the consumer's decision." Luskins, Inc. v. Consumer Prot. Div., 726 A.2d 702, 713 (Md. 1999) (citing Matter of Cliffdale Assocs., 103 F.T.C. 110, 175–76 (1984)). Where, as here, there is no evidence that a consumer was even aware of an alleged misrepresentation, there is also no basis for assuming any "probability that the deceptive practice affected the consumer's decision." Id. This conclusion, moreover, comports with cases in which courts have dismissed MCPA claims "for want of any allegation that [plaintiff] relied on [defendant's] representations to her detriment." Peete-Bey, 131 F. Supp. 3d at 433; see also Currie v. Wells Fargo Bank, N.A., 950 F. Supp. 2d 788, 798 (D.

Md. 2013) (holding that an MCPA claim could not be based on alleged misrepresentations made after the plaintiffs had entered into the agreement at issue); In re ZF-TRW Airbag Control Units Prods. Liab. Litig., 601 F. Supp. 3d 625, 775 (C.D. Cal. 2022) (dismissing consumer protection claim when the "consumer has neither seen nor heard" the alleged misrepresentation (quoting Preston v. Am. Honda Motor Co., Inc., 783 F. App'x 669, 670 (9th Cir. 2019))); Mouzon v. Radiancy, Inc., 200 F. Supp. 3d 83, 92–93 (D.D.C. 2016) (dismissing consumer protection claims, including MCPA claim, where plaintiffs did not allege "having been exposed to any misrepresentations" by defendant).

The Court recognizes that whether "a misrepresentation substantially induces a consumer's choice is *ordinarily* a question of fact for the trier of fact." Bank of Am., 822 F. Supp. 2d at 532 (emphasis added). But "ordinarily" is not "always." Here, the Court cannot conclude that a reasonable jury could find the element of reliance when there is no indication Plaintiffs were even cognizant of the alleged misrepresentations when they chose CareFirst as their health insurance or enrolled in the company's online portal. See, e.g., Pucci v. Annapolis Sailyard, Inc., No. CIV. JKB-10-2968, 2011 WL 3793762, at *1 (D. Md. Aug. 24, 2011) ("It is clear that anything said by [defendant] subsequent to the signing of the contract did not affect the [plaintiff's] 'choice of a product.'"); Shreve v. Sears, Roebuck & Co., 166 F. Supp. 2d 378, 417 (D. Md. 2001) ("The misrepresentations that plaintiffs allege refer to representations made in the Owner's Manual, which [plaintiff] read *after* he purchased the snow thrower. Any representations made in the Owner's Manual did not induce (as is required by § 13–301(9)) or deceive Shreve so that he would purchase the machine.").[14]

[14] In a footnote, CareFirst also argues that Plaintiffs did not plead their MCPA claim with sufficient particularity, as required by Federal Rule of Civil Procedure 9(b), which applies to MCPA claims that sound in fraud. MSJ 19 n.5. Plaintiffs do not address this argument (perhaps

2. MPIPA Theory

As an alternative to their misrepresentation theory, Plaintiffs allege that they have a valid claim based on violation of MPIPA, Md. Comm. Code § 14-3504, et seq., a violation of which constitutes an unfair or deceptive trade practice under the MCPA, id. § 14-3508.

MPIPA provides that a business "that owns, licenses, or maintains computerized data that includes personal information of an individual residing in the State, when it discovers or is notified that it incurred a *breach of the security of a system*, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach." Id. § 14-3504(b)(1) (emphasis added). The company must also provide notice of the breach to consumers affected by it. Id. § 14-3504(b)(2)–(3). MPIPA defines "breach of the security of a system" as "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the *personal information* maintained by a business." Id. § 14-3504(a)(1) (emphasis added). In turn, the statute at the time of the CareFirst breach defined "personal information" as "an individual's first name or first initial and last name in combination with any one or more of the following data elements"—"a Social Security Number," a "driver's license number," a "financial

---

understandably, as it is raised only in passing in a footnote). Even if this argument is not waived, however, Plaintiffs likely have just barely satisfied Rule 9(b). Rule 9(b) requires fraud claims to set out "the time, place, and contents of the false representations, as well as the identity of the person making the misrepresentation and what he obtained thereby." Harrison v. Westinghouse Savannah River Co., 176 F.3d 776, 784 (4th Cir. 1999) (quoting 5 Charles Alan Wright & Arthur R. Miller, Fed. Prac. and Proc.: Civ. § 1297, at 590 (2d ed. 1990)). "A court should hesitate to dismiss a complaint under Rule 9(b) if the court is satisfied (1) that the defendant has been made aware of the particular circumstances for which she will have to prepare a defense at trial, and (2) that plaintiff has substantial prediscovery evidence of those facts." Id. Plaintiffs' complaint identifies CareFirst's "Privacy Policy" as the source of the misrepresentation and quotes the passage at issue here. SAC ¶¶ 29, 102. Even if Plaintiffs did not identify which particular CareFirst entity is responsible for the Notice, CareFirst obviously was well equipped to identify the Notice and who issued it.

account number, including a credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account," and an "Individual Taxpayer Identification Number." Id. § 14-3501(d)(1) (effective Jan. 1, 2008 to Dec. 31, 2017).

Plaintiffs allege that CareFirst violated MPIPA by failing to conduct a timely investigation and by failing to timely notify them of the breach, which the company did not do until 2015, a year after the phishing incident. See SAC ¶ 67. CareFirst correctly contends, however, that MPIPA does not apply to this data breach because the cyberattack did not "compromise[] the security, confidentiality, or integrity of" members' Social Security numbers, financial accounts numbers, driver's license numbers, or taxpayer identification numbers. MSJ at 23. As discussed above, the undisputed record shows that Plaintiffs' Social Security numbers were not accessed in the cyberattack. Although Plaintiffs' complaint alleges that their subscriber ID numbers constitute "financial account numbers" under the statute, SAC ¶ 104, Plaintiffs do not advance this theory in their opposition. Even if Plaintiffs had not waived this argument, the Court does not construe "financial account numbers" to include Plaintiffs' subscriber ID numbers, which are merely identification numbers associated with Plaintiffs' health insurance profiles and have no connection with bank or other financial accounts. Moreover, the breach did not reveal or affect any "security code, access code, or password" that would have allowed access to the CareFirst portal in any event. Md. Comm Code § 14-3501(d)(1) (effective Jan. 1, 2008 to Dec. 31, 2017). Thus, because the data exfiltrated during the CareFirst data breach does not include any of the information specified by the statute at the time, there was no qualifying "breach of a security system" to trigger MPIPA's applicability. Id. § 14-3504.

To argue that the breach implicated MPIPA, Plaintiffs again point to the portion of this Court's and the Circuit's decisions restating the allegation that the cyberattack implicated information "that could be combined to commit identity theft and fraud." Opp'n at 20. But, as stated above, those statements were a description of the complaint's allegation that Social Security numbers were leaked, which has not been borne out by the evidence.

Additionally, Plaintiffs posit—without elaboration—that "even if Social Security numbers, driver's license numbers, financial account numbers, or Taxpayer Identification Numbers were not accessed in the CareFirst data breach, such information was still *compromised* as a result of the data breach, even if it was not directly accessed." Opp'n at 20 (emphasis in original). Although Plaintiffs' argument here is far from clear, the Court understands this sentence to suggest that the "security, confidentiality, or integrity" of their Social Security numbers has been "compromised"—i.e., weakened (as opposed to revealed to an unauthorized person)—by the breach of Plaintiffs' other information, which could subsequently be used to obtain covered personal information in the future. Id. at 19–20. If that is Plaintiffs' theory, the Court agrees that such a reading is not unreasonable. For instance, Plaintiffs' interpretation might cover a breach in which consumer names and login information (both usernames *and* passwords) were leaked, as hackers might then be able to use that information to access a consumer's online profile and steal more sensitive information covered by the statute, such as Social Security or credit card numbers. Even if that interpretation of MPIPA is plausible, however, Plaintiffs have not identified any evidence that the data accessed in this breach—member names, subscriber ID numbers, usernames, e-mail addresses, and birth dates—would give hackers ready access to Social Security numbers or financial account information

maintained by CareFirst.[15] Perhaps the leaked data could be enough to enable some forms of future mischief; perhaps not. What matters here is that Plaintiffs identify no evidence, aside from the single, speculative sentence in the Korczyk expert report described above, that the information breached here actually impacted the security of the personal information covered by MPIPA.

Moreover, even if MPIPA applied, CareFirst likely satisfied its obligations under the law. CareFirst was aware of the phishing incident when it occurred in April 2014, but based on its initial investigation (which included examining and reimaging the computers of the employees who had clicked on the malware, MSJ, Ex. C at 193), the company did not believe the incident had led to any access to its computer systems. CareFirst did not learn of the full extent of the cyberattack until April 2015, after the Mandiant investigation, and it promptly notified members of the attack at that point. In other words, CareFirst complied with MPIPA once it "discover[ed] or [was] notified of" the breach. Md. Comm. Code § 14-3504(b)(1). Plaintiffs characterize CareFirst's failure to detect the breach earlier as "willful ignorance of the strong likelihood that a breach occurred," Opp'n at 20–21, but the evidence they have produced, as discussed above, at most supports the conclusion that the company could have had particular systems in place that would have better detected the hackers' continued presence. Based on that evidence, the Court cannot say CareFirst failed to act "in good faith" in conducting its investigation when it did and not earlier. Md. Comm. Code § 14-3504(b)(1).

* * *

[15] Critically, CareFirst members' passwords were *not* a part of the data breach. MSJ, Ex. A ¶ 20.

Accordingly, because Plaintiffs have failed to point to evidence from which a reasonable jury could find they relied on CareFirst's Notice of Privacy Practices, and because MPIPA, during the relevant time, did not cover a data breach of the information leaked here, the Court grants CareFirst summary judgment as to Plaintiffs' MCPA claim.

C. Virginia Consumer Protection Act

Last, CareFirst moves for summary judgment on Plaintiffs' VCPA claim, which is premised on the same alleged misrepresentation in the Notice of Privacy Practices as their MCPA claim. Here, the analysis is even simpler. By its own text, the VCPA does not apply to Plaintiffs' claims against CareFirst.

The VCPA outlaws a number of unfair consumer practices, including misrepresenting the benefits of goods or services and using deception, fraud, or misrepresentation in consumer transactions. Va. Code Ann. § 59.1-200. The statute also provides, however, that "[n]othing in this chapter shall apply to . . . insurance companies regulated and supervised by the State Corporation Commission or a comparable federal regulating body." Id. § 59.1-199 ("Exclusions"). As the Fourth Circuit has explained, the "spectre of governmental supervision served as the legislative justification for exempting [insurance companies, banks, credit unions, and the like] from the scope of the Consumer Protection Act." Gill v. Rollins Protective Servs. Co., 773 F.2d 592, 597–98 (4th Cir. 1985), opinion amended on denial of reh'g, 788 F.2d 1042 (4th Cir. 1986).

CareFirst has provided an uncontested declaration stating that CareFirst BlueChoice, Inc., the CareFirst subsidiary operating in Virginia which had insurance contracts with the Virginia Plaintiffs, "is registered with the Virginia State Corporation Commission to conduct the business of insurance in the Commonwealth of Virginia and is subject to regulation by the Virginia

Bureau of Insurance and other agencies of the Commonwealth." MSJ, Ex. B ¶¶ 4, 11; see also DSUF ¶¶ 21–23. The Virginia Bureau of Insurance is a division of the Virginia State Corporation Commission "established to administer the insurance laws of the Commonwealth." Va. Code Ann. § 38.2-100. The Bureau "licenses, regulates, investigates and examines insurance companies, agencies and agents on behalf of the citizens of the Commonwealth of Virginia." Insurance Agents & Agencies, State Corp. Comm'n, https://www.scc.virginia.gov/pages/Bureau-of-Insurance (last visited Sept. 13, 2023). Thus, because CareFirst is an insurance company regulated by the State Corporation Commission, the VCPA does not apply to it. MSJ at 30–31.

Plaintiffs assert that CareFirst is "not exempt from Plaintiffs' VCPA claims because CareFirst's failure to protect Plaintiffs' personal information is separate and distinct from CareFirst's primary service of selling health insurance." Opp'n at 29. There is no basis for this distinction in the text of the VCPA. One of the Court's previous opinions in this case shows why. At the motion to dismiss stage, the Court rejected CareFirst's argument that a provision of the MCPA exempting from coverage the "professional services" of an "insurance company" applied to this case. Attias II, 365 F. Supp. 3d at 26 (quoting Md. Comm. Code § 13-104(1)).[16] Explaining that Maryland's highest court had interpreted "'professional services' narrowly as applied to 'medical or dental practitioner[s],' who are also exempt under the MCPA," the Court concluded "that the professional-services exemption of the MCPA does not apply to CareFirst's data-security practices," which are "ancillary to the provision of health insurance coverage much like billing is ancillary to the provision of medical care." Id. at 26–27. In other words, the

[16] The Court had no occasion to consider the VCPA's exemption provision in that opinion because it had already dismissed those claims for a failure to allege actual damages. Attias II, 365 F. Supp. 3d at 17.

"professional services" language of the MCPA's exemption provision was intended to distinguish between the "commercial or entrepreneurial" aspects of a covered profession and the aspects that go to the core of the service. Id. (quoting Scull v. Groover, Christie & Merritt, P.C., 76 A.3d 1186, 1196 (Md. 2013)). The VCPA, in contrast to the MCPA, contains no such language limiting the exemption to the "professional services" of insurance providers; it applies without qualification to "insurance companies" so long as they are "regulated and supervised by the State Corporation Commission or a comparable federal regulating body." Va. Code Ann. § 59.1-199(4).

Plaintiffs next point to a separate exclusion that exempts from VCPA coverage "[a]ny aspect of a consumer transaction which aspect is authorized under" state or federal law. Id. § 59.1-199(1). Plaintiffs maintain that the Court must therefore determine whether state or federal law authorized consumer transactions with CareFirst. Opp'n at 29. The Court agrees with CareFirst's observation that "[t]his argument makes no sense." Reply at 17 n.8. The exemption for insurance companies regulated by the State Corporations Commission is a completely separate exemption from the one excluding VCPA coverage for aspects of consumer transactions authorized under state or federal law. The exemptions are presented as separate items on a list, not as separate conditions all of which are required for an exemption to apply. The fact that one exemption does not apply is irrelevant to whether a different exemption does.

The conclusion that the VCPA's exemption applies here does not, of course, mean that CareFirst and other insurers in Virginia operate in a consumer-protection-free zone. Other provisions of Virginia law, enforced by the State Corporation Commission, prohibit health insurers from engaging in misleading advertising and provide for the suspension or revocation licenses if insurers advertise "services in an untrue, misrepresentative, misleading, deceptive, or

unfair manner." Va. Code Ann. § 38.2-4316(6); see id. § 38.2-4312; id. § 38.2-502 (generally prohibiting misrepresentations and false advertising of insurance policies). The existence of these other provisions illustrates the Fourth Circuit's observation that the "spectre of governmental supervision" over entities such as insurance companies "served as the legislative justification for exempting" them from the VCPA. Gill, 773 F.2d at 597–98. Accordingly, because the VCPA expressly carves out insurance companies regulated by the State Corporation Commission, Plaintiffs' claims under the VCPA must be dismissed.[17]

D. Timing of Summary Judgment Motion

To tie up one loose end, the Court briefly addresses Plaintiffs' contention that CareFirst's motion for summary judgment, which was filed while Plaintiffs' motion for class certification was still pending this Court's decision, is premature under Federal Rule of Civil Procedure 56(d). See Opp'n at 2–4. Specifically, Plaintiffs assert that the Court's scheduling order contemplated that additional discovery would be permitted after a decision on the class certification motion and that they need more time to "offer qualified expert testimony related to Defendants' failure to comply with HIPAA." Opp'n at 3–4.

As a general matter, a party "may file a motion for summary judgment at any time until 30 days after the close of all discovery," unless a different time is set by local rule or court order.

[17] Even if the VCPA's exemption for insurance companies were not dispositive, Plaintiffs' VCPA claim would, like their MCPA claim, fail for lack of evidence of reliance. The VCPA requires reliance on the alleged misrepresentation. Owens v. DRS Auto. Fantomworks, Inc., 764 S.E.2d 256, 260–61 (Va. 2014). In his deposition, Richard Bailey stated that CareFirst was among several plans available for him to choose as a Transportation Security Administration employee and that he did not "go out in the open marketplace and pick insurance Plan A over insurance Plan B." MSJ, Ex. L at 23. Latanya Bailey had CareFirst via her husband Richard's employment. MSJ, Ex. M at 12. Like the statements of the Maryland Plaintiffs, Mr. Bailey's description of his decision to choose CareFirst does not suggest that he relied on, or was even aware of, the Notice of Privacy Practices. And as with the MCPA claim, Plaintiffs cite no evidence to the contrary.

Fed. R. Civ. P. 56(b). The Court doubts that Plaintiffs have sustained their obligation under Rule 56(d), which requires a party seeking to defer summary judgment to (1) "outline the particular facts he intends to discover and describe why those facts are necessary to the litigation," (2) "explain 'why [he] could not produce [the facts] in opposition to the motion [for summary judgment],'" and (3) "show the information is in fact discoverable." Convertino v. U.S. Dep't of Just., 684 F.3d 93, 99–100 (D.C. Cir. 2012) (citations omitted). Here, Plaintiffs' opposition offers only a vague suggestion that they need more time to "offer qualified expert testimony related to Defendants' failure to comply with HIPAA," Opp'n at 4, and their supporting affidavit does not provide even that level of detail.

In any case, the Court need not decide whether Plaintiffs' request for relief under Rule 56(d) might warrant deferral of summary judgment. As explained above, even without any additional expert discovery on HIPAA compliance, the Court denies CareFirst's motion for summary judgment as to Plaintiffs' breach of contract claim. And the Court grants summary judgment as to Plaintiffs' MCPA and VCPA claims for reasons unrelated to CareFirst's compliance with HIPAA. Whether Plaintiffs might obtain additional expert opinions regarding CareFirst's HIPAA compliance therefore has no bearing on the outcome of this motion.

IV. Conclusion

For these reasons, it is hereby

ORDERED that [Dkt. No. 94] Defendant's Motion for Summary Judgment is GRANTED in part and DENIED in part.

SO ORDERED.

CHRISTOPHER R. COOPER
United States District Judge

Date: September 13, 2023