**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| VIRGINIA ANDERSON, *et al.*,<br>*Plaintiffs*,<br>v.<br>FUNDAMENTAL ADMINISTRATIVE SERVICES, LLC, *et al.,*<br>*Defendants*. | Case No. 25-cv-2754-ABA |

**MEMORANDUM OPINION AND ORDER**

Plaintiffs Virginia Anderson, Willie Kirkland, and Brian Thompson, individually and on behalf of putative class members, contend that Defendants Fundamental Administrative Services, LLC ("Fundamental"), Crimson Heights Health and Wellness ("Crimson Heights"), and Horizon Health & Rehabilitation Center ("Horizon") (collectively, "Defendants") are responsible for a data breach that resulted in the theft of Plaintiffs' protected health information ("PHI"). Defendants have moved to dismiss the consolidated class action complaint. For the following reasons, the Court will deny the motion to dismiss with the exception that it will dismiss the claims no longer pursued by Plaintiffs.

## I. FACTS[1]

Crimson Heights is a nursing facility in Texas that provides short-term and long-term care, physical rehabilitation, memory care, and 24-hour nursing care services. ECF No. 24 ¶ 5. Horizon is a nursing facility located in Nevada that offers short-term and

[1] At the pleadings stage, the Court must "accept as true all of the factual allegations contained in the complaint and draw all reasonable inferences in favor of the" non-movant. *King v. Rubenstein*, 825 F.3d 206, 212 (4th Cir. 2016).

long-term care, physical rehabilitation, respiratory care, wound care programs, physician services, 24-hour nursing care services, and other programs. *Id.* ¶ 6. Crimson Heights and Horizon are referred to herein as the "Health Care Defendants." Anderson and Kirkland are Texas residents; they are or were patients of Crimson Heights.[2] Thompson is a Nevada resident and was a patient of Horizon.

Plaintiffs allege that, in order to receive services from the Healthcare Defendants, they were required to provide them their PHI, including their names, dates of birth, driver's license numbers, Social Security numbers, financial account information, medical treatment information, health insurance and Medicaid/Medicare information, and other sensitive data.

Plaintiffs describe Fundamental as "a nationwide health care services company headquartered in Sparks, Maryland." *Id.* ¶ 4. The complaint provides little to no detail on the nature of the services that Fundamental provided to Crimson Heights and Horizon. The complaint alleges that Fundamental "operates and manages . . . nursing homes and rehabilitation centers." *Id.* Fundamental says that misconstrues its role: it "neither manages nor operates" such entities. ECF No. 30-1 at 10 n.1. But that dispute is for another day: regardless of the scope of services that Crimson Heights and Horizon engaged Fundamental to provide, Plaintiffs allege that relationship required Fundamental to obtain access to the PHI of the Healthcare Defendants' patients. ECF No. 24 ¶ 38. Plaintiffs allege that one of Fundamental's duties, both to the Healthcare Defendants and the patients, was to safeguard those patients' private data.

---

[2] At the time of the amended complaint, Kirland was a then-"current resident of Crimson Heights." ECF No. 24 ¶ 192.

On January 20, 2025, Fundamental discovered that its networks had been breached between October 27, 2024 and January 13, 2025, a breach that included the PHI of the Healthcare Defendants' patients, including Plaintiffs' PHI (the "Data Breach").

Plaintiffs allege that, as a result of the Data Breach, they fear they will be the victims of future fraud and identity theft, resulting in emotional distress and anxiety. They also allege that they have lost time and resources attempting to mitigate the risk of identity fraud, that their private information now has diminished value, and that they have suffered a loss of privacy. Additionally, Anderson alleges that after the Data Breach she was notified by her bank that someone attempted (unsuccessfully) to purchase $500 worth of furniture in Spain by charging it to her account. Anderson also alleges that she has received an increased volume of spam emails. Thompson additionally alleges that he has received multiple notifications from credit monitoring services informing him that his PHI has been found on the dark web, and he claims to have experienced a sharp uptick in suspicious spam calls, texts, and emails, which he attributes to the Data Breach.

On November 14, 2025, Plaintiffs filed a consolidated class action complaint. ECF No. 24. Through briefing and during oral argument, Plaintiffs have revised the claims made against the Defendants and currently assert three counts:

Count I – Negligence against all Defendants

Count II – Breach of implied contract against the Healthcare Defendants

Count III – Unjust enrichment against the Healthcare Defendants[3]

---

[3] All other claims originally sought in the complaint have been abandoned by Plaintiffs, and will be dismissed.

Defendants moved to dismiss the complaint pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(2), and 12(b)(6). ECF No. 30. Plaintiffs responded, and Defendants replied. ECF Nos. 36, 38. The Court held a hearing on August 3, 2026.

## II. STANDARDS

### A. Rule 12(b)(1)

"A motion to dismiss based on lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1) raises the question of whether the court has the competence or authority to hear the case." *Davis v. Thompson*, 367 F. Supp. 2d 792, 799 (D. Md. 2005). In this case, Defendants allege that Plaintiffs lack standing to bring the action before this Court. "The burden of establishing subject matter jurisdiction is on . . . the party asserting jurisdiction." *Robb Evans & Assocs., LLC v. Holibaugh*, 609 F.3d 359, 362 (4th Cir. 2010). A Rule 12(b)(1) motion "must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction." *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009).

### B. Rule 12(b)(2)

"Under Rule 12(b)(2), a defendant must affirmatively raise a personal jurisdiction challenge, but the plaintiff bears the burden of demonstrating personal jurisdiction at every stage following such a challenge." *Grayson v. Anderson*, 816 F.3d 262, 267 (4th Cir. 2016). "[A] Rule 12(b)(2) challenge raises an issue for the court to resolve, generally as a preliminary matter." *Id.* "[W]hen the court addresses the personal jurisdiction question by reviewing only the parties' motion papers, affidavits attached to the motion, supporting legal memoranda, and the allegations in the complaint, a plaintiff need only make a *prima facie* showing of personal jurisdiction to survive the jurisdictional challenge." *Id.* at 268. "When determining whether a plaintiff has made the requisite *prima facie* showing, the court must take the allegations and available evidence relating to personal jurisdiction in the light most favorable to the plaintiff." *Id.* In other words, "[u]nlike under Rule 12(b)(6), the court may . . . consider affidavits submitted by both parties, although it must resolve all factual disputes and draw all reasonable inferences in favor of the party asserting jurisdiction." *Hawkins v. i-TV Digitalis Tavkozlesi zrt.*, 935 F.3d 211, 226 (4th Cir. 2019).

**C. Rule 12(b)(6)**

A complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). When a defendant asserts that, even assuming the truth of the alleged facts, the complaint fails "to state a claim upon which relief can be granted," the defendant may move to dismiss the complaint. Fed. R. Civ. P. 12(b)(6). To withstand a motion to dismiss, the complaint's "[f]actual allegations must be enough to raise a right to relief above the speculative level" and state a facially plausible claim for relief. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). As stated, when considering such a motion, the Court must "accept as true all of the factual allegations contained in the complaint and draw all reasonable inferences in favor of the plaintiff." *King*, 825 F.3d at 212. "[T]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678. The Court is "not bound to accept as true a legal conclusion couched as a factual allegation." *Id.* (quoting *Twombly*, 550 U.S. at 555).

## III. DISCUSSION

Defendants argue that (1) the Court lacks subject matter jurisdiction because Plaintiffs lack standing to bring the case; (2) the Court lacks personal jurisdiction over the Healthcare Defendants; and (3) Plaintiffs' claims fail to state claims upon which relief can be granted.

### A. Standing/Subject Matter Jurisdiction

"[T]o establish standing, a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021).

Defendants contend that Plaintiffs (Anderson, Kirkland, and Thompson) lack standing primarily because they have not alleged adequate injury-in-fact. The "mere compromise of personal information, without more, fails to satisfy the injury-in-fact element [for standing] in the absence of an identity theft." *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018). To establish standing in the context of a data breach, a plaintiff must allege "a nonspeculative increased risk of identity theft," *O'Leary v. TrustedID, Inc.*, 60 F.4th 240, 244 (4th Cir. 2023), that is "sufficiently imminent." *Hutton*, 892 F.3d at 621. "In a class action, [courts] analyze standing based on the allegations of personal injury made by the named plaintiffs"; "[w]ithout a sufficient allegation of harm to the named plaintiff in particular, plaintiffs cannot meet their burden of establishing standing." *Beck v. McDonald*, 848 F.3d 262, 269–70 (4th Cir. 2017) (quoting *Doe v. Obama*, 631 F.3d 157, 160 (4th Cir. 2011)). But "[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we 'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990)).

Plaintiffs contend they have satisfied these standards—in particular, the requirement that they allege that they each now face "a nonspeculative increased risk of identity theft," *O'Leary*, 60 F.4th at 244—for several reasons, including that Plaintiffs have alleged that their PHI that was stolen during the breach of Fundamental's systems now appears on the "dark web." ECF No. 24 ¶ 21 ("Upon information and belief, Plaintiffs' Private Information is available on the dark web as a result of the Data Breach."); *id.* ¶ 26 ("Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web."); *id.* ¶ 171 ("[S]ince the Data Breach, Plaintiffs have received multiple notifications from different credit monitoring and financial services that their compromised Private Information has been published on the dark web."); *id.* ¶ 199 (Kirkland's PHI, "on information and belief . . . has been sold for [criminal, fraudulent] purposes and posted on the dark web for sale"); *id.* ¶ 214 ("Thompson has received multiple notifications from Experian, CreditWise, and IDX credit monitoring services informing him that his compromised Private Information has been found published on the dark web."). Anderson also alleges that after the Data Breach her bank informed her that someone attempted to use her credit card, and Anderson and Thompson both allege they have received an increased number of spam communications that they attribute to the Breach. *Id.* ¶¶ 186, 190, 216.

The Court concludes that the first allegation listed above—specifically that Plaintiffs' PHI was made available on the dark web due to the Data Breach, ECF No. 24 ¶¶ 21, 26, 171, 199, 214—which Plaintiffs have alleged affects each of them, is sufficient to satisfy Plaintiffs' burden to allege that the Data Breach caused them an injury-in-fact beyond the "mere compromise of personal information," *Hutton*, 892 F.3d at 621. The Fourth Circuit has held that alleging that personal information has been made available on the dark web due to a data breach is adequate injury-in-fact for standing purposes. *Holmes v. Elephant Ins. Co.*, 156 F.4th 413, 425–26 (4th Cir. 2025) (Plaintiffs "allege that they found their driver's license numbers listed on the dark web and attribute the listings to the Elephant breach," which "is sufficient to show a concrete injury in the eyes of Article III"), *cert. dismissed*, 146 S. Ct. 2549 (2026). That is because this sort of disclosure of personal and confidential information over the dark web is akin to the traditionally recognized harm of public disclosure of private information. *Id.* at 423–24. Given these allegations, Plaintiffs have adequately alleged injury-in-fact for standing purposes.

Beyond injury-in-fact, to establish standing Plaintiffs must also allege that those injuries were caused by Defendants and that those injuries would be redressable by judicial relief. *TransUnion LLC*, 594 U.S. at 423. Defendants argue that Plaintiffs' allegations regarding the causation of their injuries is conclusory. ECF No. 30 at 18–19. But district courts in the Fourth Circuit "have routine[ly] found traceability in the data breach context where plaintiffs provided defendants with [personally identifiable information ('PII')] and those defendants subsequently fell victim to a targeted data breach resulting in the disclosure and misuse of plaintiffs' PII." *Gordon v. Zeroed-In Tech., LLC*, Case No. 23-cv-3284-BAH, 2025 WL 936415, at *9 (D. Md. Mar. 26, 2025) (quoting *Capiau v. Ascendum Mach., Inc.*, Case No. 3:24-cv-00142-MOC-SCR, 2024 WL 3747191, at *7 (W.D.N.C. Aug. 9, 2024)) (citing cases).

The Court concludes that Plaintiffs' causation allegations—that they provided their PHI to the Defendants and were injured when that information was stolen in the Data Breach, ECF No. 24 ¶¶ 1, 23, 27, 44, 123–77—are sufficient to allege causation for standing purposes at this stage. But "each element [of standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation." *Lujan*, 504 U.S. at 561. Thus, Plaintiffs will continue to have the burden to establish standing (along with each element of their claims on the merits) as the case progresses.

### B. Specific Personal Jurisdiction

The Healthcare Defendants, which as noted above are located in Texas and Nevada, argue that this Court lacks personal jurisdiction over them. To determine whether the exercise of specific jurisdiction over a defendant is constitutional (Plaintiffs here do not invoke general personal jurisdiction), courts "consider (1) the extent to which the defendant purposefully availed itself of the privilege of conducting activities in the State; (2) whether the plaintiffs' claims arise out of those activities directed at the State; and (3) whether the exercise of personal jurisdiction would be constitutionally reasonable." *Consulting Eng'rs Corp. v. Geometric Ltd.*, 561 F.3d 273, 278 (4th Cir. 2009) (quoting *ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, 293 F.3d 707, 712 (4th Cir. 2002)).

Plaintiffs have adequately alleged facts giving rise to specific personal jurisdiction over the Healthcare Defendants. The Healthcare Defendants hired

Fundamental to provide services that involved the Healthcare Defendants transmitting PHI about their patients to Fundamental. ECF No. 24 ¶ 38. Fundamental is located in Maryland, and the amended complaint as a whole alleges that the services that the Healthcare Defendants hired Fundamental to provide—including services that entailed receipt of patients' PHI—were performed by Fundamental employees located in Maryland. *See, e.g.*, *id.* ¶¶ 3–4, 7, 32, 38, 44.

Accepting these allegations as true and drawing all reasonable inferences in Plaintiffs' favor, as the Court must do at the pleadings stage, those contacts between the Healthcare Defendants and Maryland satisfy the purposeful availment prong of the specific jurisdiction standard. Adequate personal availment can be shown when "the defendant reached into the forum state to solicit or initiate business," and also in the face of "the performance of contractual duties . . . within the forum." *Consulting Eng'rs Corp.*, 561 F.3d at 278. In addition, Plaintiffs' data-breach claims arise from services provided by Fundamental, allegedly in Maryland; their claims are based on alleged injuries sustained when Fundamental's systems were breached and Plaintiffs' PHI was stolen, which had been provided to Fundamental by the Healthcare Defendants. *See, e.g.*, *id.* ¶ 38 (alleging that the Healthcare Defendants provided Plaintiffs' PHI to Fundamental for administration and data management). Therefore, the Court concludes that the exercise of specific personal jurisdiction over the Healthcare Defendants is appropriate and satisfies due process.

### C. Negligence

Plaintiffs have sued all three defendants for negligence (Count I), alleging that Fundamental, Horizon, and Crimson Heights owed Plaintiffs and putative class members a duty to "exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their and/or their service providers' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons," ECF No. 24 ¶ 116, a duty that Plaintiffs allege each Defendant breached by "fail[ing] to take the necessary precautions to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure," *id.* ¶ 122. Defendants argue that Plaintiffs' negligence claim fails to state a claim on which relief can be granted for several reasons. Before addressing the merits of those arguments, however, the Court first addresses a threshold question of which state's or states' laws governed Defendants' common law duties to Plaintiffs.

**1. Choice of Law**

As noted, Defendants argue that Plaintiffs have failed to adequately plead a negligence claim. "The conflict of laws rules to be applied by the federal court in [a state] must conform to those prevailing in [that state's] courts." *Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496 (1941)). So, Maryland's choice of law rules apply here. For tort cases, "Maryland applies the *lex loci delicti* rule," which provides that "when a tort occurs in another state, the substantive rights of the parties, even though they are domiciled in Maryland, are to be determined by the law of the state in which the alleged tort took place." *Id.* (citing *Philip Morris, Inc. v. Angeletti*, 358 Md. 689 (2000)). Under that rule, "[a] tort occurs 'where the injury was suffered, not where the wrongful act took place.'" *Id.* at 480–81 (quoting *Johnson v. Oroweat Foods Co.*, 785 F.2d 503, 511 (4th Cir. 1986)).

Defendants contend that to the extent Anderson and Kirkland were injured, their injuries were suffered in Texas, and Thompson's injuries were in Nevada. Plaintiffs do not dispute this choice-of-law analysis or otherwise articulate any different law that would govern Plaintiffs' claims.[4] Accordingly, Texas law applies to Anderson's and Kirkland's negligence claims, and Nevada law applies to Thompson's negligence claims. Texas and Nevada share the same elements for negligence: (1) a legal duty owed by defendant to plaintiff; (2) a breach of that duty, and (3) damages proximately caused by the breach. *Lee Lewis Constr., Inc. v. Harrison*, 70 S.W.3d 778, 782 (Tex. 2001); *Clark Cnty. Sch. Dist. v. Payo*, 403 P.3d 1270, 1279 (Nev. 2017).

**2. Damages**

Defendants argue that Plaintiffs have not alleged the damages required for a negligence claim. But, under Texas law, courts have held that plaintiffs sufficiently alleged negligence damages when they alleged "that as a result of the data breach, their PII has been sold or exposed on the dark web, and they have suffered an increased risk of future harm." *Hawkins v. Scout Energy Mgmt., LLC*, Case No. 3:24-cv-01545-N, 2025 WL 2244327, at *8 (N.D. Tex. Aug. 5, 2025). As discussed above in the context of deciding whether Plaintiffs have standing, Anderson and Kirkland have made these allegations.

Under Nevada law, Defendants contend that Thompson cannot show damages arising from, among other things, exposure of his PHI on the dark web unless he can

---

[4] Plaintiffs do contend that applying a choice-of-law analysis is "premature." ECF No. ECF No. 36 at 19. But Defendants have moved to dismiss in part by arguing that Plaintiffs' state-law claims do not state claims on which relief can be granted. That requires identifying the applicable law. There may not be a *conflict* between the potentially applicable laws when it comes to the elements of a negligence claim—and thus the present motion may not require an actual "choice" of law—but the nature of Defendants' motion does require that the Court identify the universe of potential state laws that may govern Plaintiffs' claims. Here, the only states' laws that either side has suggested apply to Plaintiffs' claims are the laws of Texas and Nevada (where the facilities where Plaintiffs were patients are located).

show that his PHI is now less valuable. *See Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1234–35 (D. Nev. 2020), *aff'd,* 845 F. App'x 613 (9th Cir. 2021) (reasoning that "[d]iminution in the value of personal information can be a viable theory of damages" but only if "the plaintiff has been unable to sell, profit from, or otherwise monetize her personal information"). But *Pruchnicki*'s reasoning was rejected in *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1190 (D. Nev. 2022) ("[T]hese pleading requirements, that Plaintiffs must establish both the existence of a market for their PII and an impairment of their ability to participate in that market, is not supported by Ninth Circuit precedent and other district courts in this Circuit have rejected them" and instead holding that a plaintiff may plead damages for a negligence claim by "alleg[ing] details about the existence of an economic market for selling stolen PII, including the fact that PII can be bought and sold at identifiable prices on established markets"). *See also In re Anthem, Inc. Data Breach Litig.*, Case No. 15-md-02617-LHK, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) (observing that under California law, a plaintiff must "allege that there was either an economic market for their PII or that it would be harder to sell their own PII, not both"). Plaintiffs, including Thompson, have alleged diminution in the value of their PHI, that markets for stolen PHI exist, and specific values for that information. ECF No. 24 ¶¶ 78, 130, 133, 163–69, 249. Regardless, the court in *Smallman* also found negligence damages allegations to be adequate under Nevada law where the plaintiffs alleged that their "PII has already been posted for sale or used in attempt identity theft attacks" because it "sufficiently show[ed] that the PII stolen creates a substantial risk of future harm." 638 F. Supp. 3d at 1191.

For the purposes of this motion to dismiss, the Court concludes that Plaintiffs have adequately alleged damages to support their negligence claims.

### 3. Existence of a Duty by Fundamental

In their briefs and during oral argument, the parties asserted that Maryland law controls whether Fundamental owed a duty to Plaintiffs and do not make any duty-related arguments under Nevada or Texas law. ECF No. 30 at 27; ECF No. 36 at 19. For purposes of this opinion, the Court will accept that proposition, although it may not ultimately be correct if the Court were required to perform a full choice of law analysis. Defendants argue that Plaintiffs fail to allege what specific duty Fundamental owed them and note that while Plaintiffs had relationships with the Healthcare Defendants, who had a relationship with Fundamental, the Plaintiffs themselves did not have a relationship or privity with Fundamental directly. Under Maryland law, "[w]here the failure to exercise due care creates a risk of economic loss only," as Defendants allege is the case here, "courts have generally required an intimate nexus between the parties as a condition to the imposition of tort liability," which can be "satisfied by contractual privity or its equivalent." *Chicago Title Ins. Co. v. Allfirst Bank*, 394 Md. 270, 291 (2006) (quoting *Noble v. Bruce*, 349 Md. 730, 739–40 (1998)).

But, even if Plaintiffs' only cognizable damages are economic, the Court concludes that Plaintiffs' allegations are sufficient to avoid dismissal under the economic loss doctrine under Maryland law, at least at the pleadings stage. Defendants are correct that there is no privity between Fundamental and Plaintiffs. But there is a privity equivalent—an intimate nexus—at least accepting Plaintiffs' allegations as true, as the Court must do at the pleadings stage: Plaintiffs allege that Fundamental knew or should have known that Plaintiffs were relying on it to keep their PHI secure. The "privity-equivalent analysis in economic loss cases looks for linking conduct—enough to show the defendant knew or should have known of the plaintiff's reliance," which means that "context is critical." *Balfour Beatty Infrastructure, Inc. v. Rummel Klepper & Kahl, LLP*, 451 Md. 600, 620–21 (2017). While Maryland courts have not spoken widely on the issue, at least two courts in this district applying Maryland law have concluded in factually similar situations that an intimate nexus existed.

*In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, involved negligence claims against a data management company (Accenture) for a data breach of hotel customers' PII that a hotel chain had made available to Accenture. Case No. 19-cv-2879-PWG (MDL No. 19-md-2879), 2020 WL 6290670, at *1–*2 (D. Md. Oct. 27, 2020). The court discussed the application of the economic loss doctrine under Maryland law and concluded that "plaintiff[s] and defendant were sufficiently close to justify finding a tort duty running from the defendant to the plaintiff[s]," because the data management company "knew or should have known that these Plaintiffs were foreseeable victims who relied on" its obligation to use reasonable care in protecting their data. *Id.* at *6–*7. The court relied on the facts that there was a contract between Accenture and the hotel chain acknowledging a duty to protect end-users' PII and a public acknowledgement by Accenture of the possibility of liability in the event of a data breach. *Id.*

Similarly, in *Gordon*, the court held that under Maryland law, an intimate nexus existed between a data management company and employees of a retail store that had provided the employees' PII to the data management company. That was because the data management company should have known of the plaintiffs' reliance in light of, among other things, the data management company's privacy policy that acknowledged the importance of safeguarding the PII. 2025 WL 936415, at *11. The existence of the policy supported the plaintiffs' allegations that the data management company was aware of its obligation to keep the PII secure, and knew that a data breach could result in injury to the plaintiffs, but failed to secure that data. *Id.*

Here too, Plaintiffs allege that Fundamental has a Notice of Privacy Practices that "expressly affirms Defendants' legal obligations with respect to Plaintiffs' and Class Members' Private Information" and "states the specific circumstances in which Private Information may be disclosed, none of which include disclosure to unauthorized cybercriminals as in this Data Breach," indicating that Fundamental also understood it had a duty to keep such information secure. ECF No. 24 ¶ 49; *see id.* ¶ 256 (alleging that "Fundamental's Notice of Privacy Practices" obligates Fundamental "to maintain the privacy and confidentiality of the Private Information they collected and to keep such information safeguarded against unauthorized access and disclosure"). The allegations are sufficient for current purposes to show that Fundamental should have known that Plaintiffs would rely on Fundamental to keep their data private and secure. Likewise, Plaintiffs have alleged that Fundamental knew that it needed to protect the PHI because it was highly sought after by persons seeking to misappropriate it. *Id.* ¶¶ 43, 69–82. Therefore, the Court concludes that Plaintiffs have adequately alleged that there was a sufficiently close nexus between Plaintiffs and Fundamental to give rise to a duty to Plaintiffs, at least sufficient for Plaintiffs' claims to survive Fundamental's motion to dismiss on this basis. Whether the evidence will be sufficient to survive summary judgment will be a separate question that will be addressed based on the record at that time.

### 4. Breach of Duty by the Healthcare Defendants

The Healthcare Defendants argue that regardless of whether Plaintiff has alleged that *Fundamental* breached a duty of care, Plaintiffs have not alleged that *the*

*Healthcare Defendants* breached any duties; Plaintiffs do not allege the Healthcare Defendants' computer systems were hacked or that they could have stopped the cyberattack on Fundamental. ECF No. 28 at 28. Plaintiffs counter that the Healthcare Defendants breached a duty when they failed to ensure that their vendors and affiliates maintained adequate security of the PHI provided by the Healthcare Defendants to Fundamental. *See id.* ¶¶ 56, 235, 247. Accepting Plaintiffs' factual allegations as true and drawing all inferences in the light most favorable to them, the Court concludes that Plaintiffs have adequately alleged that the Healthcare Defendants breached a duty of care regarding the selection of Fundamental to keep their PHI secure. Plaintiffs will ultimately be required to prove such a breach including that it was reasonably foreseeable to the Healthcare Defendants that Fundamental's system would be breached and that Plaintiffs' PHI would be stolen.

### D. Breach of Implied Contract

Plaintiffs contend that when they "provided their Private Information and/or payment to [the Healthcare] Defendants, they formed implied contracts pursuant to which [the Healthcare] Defendants agreed to safeguard and protect such Private Information." *Id.* ¶ 254.

#### 1. Choice of Law

Maryland has adopted the doctrine of *lex loci contractus* when choosing the applicable law for a breach of contract claim. *Cunningham v. Feinberg*, 441 Md. 310, 326 (2015). "Under this principle, the law of the jurisdiction where the contract was made controls its validity and construction." *Konover Prop. Tr., Inc. v. WHE Assocs., Inc.*, 142 Md. App. 476, 490 (2002) (quoting *Kramer v. Bally's Park Place, Inc.*, 311 Md.

387, 390 (1988)). "For choice-of-law purposes, a contract is made where the last act necessary to make the contract binding occurs." *Id.*

Defendants assert that because Plaintiffs allege that when they "provided their Private Information and/or payment to Defendants, they formed implied contracts," ECF No. 24 ¶ 254, those alleged contracts were formed in Texas and Nevada where the Plaintiffs obtained services from the Healthcare Defendants. Plaintiffs do not contend otherwise. For the purposes of this opinion, the Court will accept this proposition and apply Texas law to Anderson's and Kirkland's contract claims and Nevada law to Thompson's contract claims.

Under both states' laws, a breach of contract claim requires (1) a valid contract, (2) performance by the parties, (3) material breach, and (4) damages. *Greenstein v. Wells Fargo Bank, N.A.*, 746 F. App'x 637, 638 (9th Cir. 2018) (Nevada law); *Smith Int'l, Inc. v. Egle Grp., LLC*, 490 F.3d 380, 387 (5th Cir. 2007) (Texas law). The elements are the same whether the contract is express or implied, but "[a] contract is implied when its terms arise from the acts and conduct of the parties" rather than from express terms. *E-Learning LLC v. AT & T Corp.*, 517 S.W.3d 849, 858 (Tex. App. 2017); *Certified Fire Prot. Inc. v. Precision Constr.*, 283 P.3d 250, 256 (Nev. 2012) ("A contract implied-in-fact must be manifested by conduct.") (internal quotation marks omitted).

**2. Damages**

Defendants first argue that Plaintiffs have failed to adequately show that Defendants' alleged breach of an implied contract to safeguard Plaintiffs PHI caused any cognizable harm to Plaintiff. But as discussed above, Plaintiffs have adequately pled damages for their negligence claims, which are the same damages alleged here, and courts in Texas and Nevada have declined to dismiss implied contract claims in data breach cases like this. *Hawkins*, 2025 WL 2244327, at *7–*8 (Texas law); *Cabezas v. Mr. Cooper Grp. Inc.*, Case No. 3:23-cv-2453-N, 2025 WL 2053287, at *10 (N.D. Tex. July 22, 2025); *Smallman*, 638 F. Supp. 3d at 1195 (Nevada law); *In re Data Breach Sec. Litig. Against Caesars Ent., Inc.*, Case No. 2:23-cv-01447-ART-BNW, 2025 WL 2393024, at *9 (D. Nev. Aug. 15, 2025). At this early stage of the case, Plaintiffs have pled adequate damages for their breach of implied contract claims.

### 3. Consideration

Second, Defendants contend there was no consideration for the alleged implied contracts because "a promise to fulfill a duty imposed by law is not valid consideration." *United States v. McBride*, 571 F. Supp. 596, 605 (S.D. Tex. 1983); *see also Cain v. Price*, 415 P.3d 25, 28 (Nev. 2018) ("A party's affirmation of a preexisting duty is generally not adequate consideration to support a new agreement."). Defendants argue that, as Plaintiffs allege, Defendants owed a statutory duty to protect their PHI as evidenced by the Health Insurance Portability and Accountability Act and the Federal Tort Claims Act, *see* ECF No. 24 ¶¶ 242, 258, and that an alleged implied contract is not supported by consideration that constitutes Fundamental's promise to do what the law required. The argument is that Defendants provided no consideration when they agreed to safeguard the PHI because they were already required by law to protect the data.

But Plaintiffs allege that the consideration at issue was not just the promise to fulfill a duty but also included Plaintiffs supplying their PHI to the Healthcare Defendants and Defendants providing services to Plaintiffs, both of which have value. *See id.* ¶¶ 253–54; *see also Envolve Pharmacy Sols., Inc. v. Rite Aid Headquarters Corp.*, Case No. N19C-12-214 PRW CCLD, 2023 WL 2547994, at *14 (Del. Super. Ct. Mar. 17, 2023) ("the Court views this personally identifiable information as sufficient consideration to create a valid contract."); *Perry v. Bay & Bay Transportation Servs., Inc.*, 650 F. Supp. 3d 743, 757 (D. Minn. 2023) ("Bay & Bay provided consideration by promising to consider Perry for employment, while Perry provided consideration by providing valuable property, his PI."). Even if Defendants were required under the law to secure Plaintiffs' private information, Plaintiffs provided something of value to Defendants (the PHI) and Defendants provided services in exchange, including expending resources on attempting to protect the PHI. The Court concludes that Plaintiffs have adequately pled consideration for their beach of implied contract claim against the Healthcare Defendants, at least for the purposes of the motion to dismiss.

**E. Unjust Enrichment**

Plaintiffs allege that by providing the Healthcare Defendants with their PHI, they conferred a benefit on the Healthcare Defendants that unjustly enriched them. Plaintiffs allege that "[t]he monies Plaintiffs and Class Members paid to Defendants included a premium for Defendants' cybersecurity obligations and were supposed to be used by Defendants, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiffs' and Class Members' Private Information," but "[i]nstead of providing a reasonable level of security that would have prevented the Data Breach, Defendants calculated to increase their own profits at Plaintiffs' and Class Members' expense by using cheaper, ineffective measures and diverting those funds to Defendants' own coffers." ECF No. 24 ¶¶ 270–71; *see also id.* ¶¶ 268–269, 274.

Under Nevada law, unjust enrichment requires allegations that "the plaintiff confers a benefit on the defendant, the defendant appreciates such benefit, and there is acceptance and retention by the defendant of such benefit under such circumstances that it would be inequitable for him to retain the benefit without payment of the value thereof." *Nautilus Ins. Co. v. Access Med., LLC*, 482 P.3d 683, 688 (Nev. 2021) (quoting *Cert. Fire Prot. Inc. v. Precision Constr.*, 283 P.3d 250, 257 (Nev. 2012)). Defendants argue that under Texas law, Plaintiffs must additionally allege fraud, duress, or taking of an undue advantage. *See Sullivan v. Leor Energy, LLC*, 600 F.3d 542, 550 (5th Cir. 2010) ("A plaintiff may recover under an unjust enrichment theory 'when one person has obtained a benefit from another by fraud, duress, or the taking of an undue advantage.'") (quoting *Heldenfels Bros. v. City of Corpus Christi*, 832 S.W.2d 39, 41 (Tex. 1992)).

But the holdings in *Sullivan* and *Heldenfels* did not hinge on whether there was fraud, etc. and this Court agrees with the Court of Appeals of Texas "that fraud, duress or the taking of an undue advantage is not an element of unjust enrichment, even though the doctrine is typically found to apply under one of these scenarios." *Walker v. Walker*, 631 S.W.3d 259, 266 (Tex. App. 2020) (internal quotation marks omitted); *see also Bransom v. Standard Hardware, Inc.*, 874 S.W.2d 919, 927 (Tex. App. 1994) ("A right of recovery under unjust enrichment is essentially equitable and does not depend upon the existence of a wrong."); *Oxford Fin. Companies, Inc. v. Velez*, 807 S.W.2d 460, 465 (Tex. App. 1991) ("[A] party's right to recover under a theory of unjust enrichment does not depend on the other party's commission of a wrongful act.").

Regarding Thompson's claim, Defendants argue that under Nevada law, unjust enrichment is not available where the injured party has an adequate remedy at law and does not need to resort to equity. ECF No. 30-1 at 36; *see In re Wal-Mart Wage & Hour Emp. Pracs. Litig.*, 490 F. Supp. 2d 1091, 1125 (D. Nev. 2007). Defendants contend that Plaintiffs have not alleged that there are no adequate legal remedies available for their alleged losses. *See Smallman*, 638 F. Supp. 3d at 1197 ("Plaintiffs . . . may plead unjust enrichment in the alternative to legal claims. However, '[t]he issue is not whether a pleading may seek distinct forms of relief in the alternative, but rather whether a prayer for equitable relief states a claim if the pleading does not demonstrate the inadequacy of a legal remedy.'") (quoting *Sharma v. Volkswagen AG*, 524 F. Supp. 3d 891, 907 (N.D. Cal. 2021)).

Plaintiffs counter that courts applying Nevada law to data breach cases have permitted claims for unjust enrichment to proceed when a company accepts money and fails to safeguard bargained-for data security. *See, e.g. In re Eureka Casino Breach Litig.*, Case No. 2:23-cv-00276-CDS-BNW, 2024 WL 4253198, at *9 (D. Nev. Sept. 19, 2024) ("A business can certainly expect payment in receipt for its products and services, but when part of that payment was made in exchange for protection of private information, as the plaintiffs allege here, a business has been unjustly enriched if it fails to erect those protections.").

At this stage of the case, the Court concludes that Plaintiffs have adequately alleged an unjust enrichment claim, at least as an alternative should other legal remedies prove inadequate.

## VI. CONCLUSION AND ORDER

For the reasons stated, it is ORDERED that Defendant's motion to dismiss (ECF No. 30) is GRANTED in part and DENIED in part.

The motion is GRANTED to the extent that the negligence per se claim against all Defendants in Count I, Count IV for declaratory judgment, and the claims against Fundamental in Counts II and III are DISMISSED without prejudice, as Plaintiffs have asserted that they are no longer pursuing those claims.

The motion is DENIED in all other respects.

Date: September 14, 2026

_______/s/_______________

Adam B. Abelson
United States District Judge