IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
District Judge Gordon P. Gallagher

Civil Action No. 24-cv-02939-GPG-CYC

KAREN ALEXANDER, individually and on behalf of her Minor Children,
DEIDRA DONOHOE,
JESSICA KLARIN,
JENNIFER ELLIOT,
KENNETH SMITH,
JORDAN KRISTOFF,
WILLIAM RICHARDSON, JR.,
CHRISTIAN CASTLE, and
EMMANUEL HOLGUIN, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

SUMMIT PATHOLOGY LABORATORIES, INC., d/b/a SUMMIT PATHOLOGY,

Defendant.

ORDER

Before the Court is Defendant's Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint and Motion to Strike Class Allegations (D. 29). The Court GRANTS IN PART and DENIES IN PART the motion for the following reasons.

I. BACKGROUND

This civil action arises from a data breach at Defendant Summit Pathology Laboratories, Inc. (Summit).[1] Summit is a pathology laboratory that performs laboratory tests for medical

[1] The Court draws the operative facts as set forth in the Consolidated Class Action Complaint (Complaint) (D. 13). Consistent with the standard, the Court presumes the well pleaded factual allegations are true for the purposes of this motion.

providers in Colorado, Wyoming, and Nebraska. In relation to it business, Summit collects and generates a variety of information about medical patients. This information is stored by Summit and includes contact information, identity information, financial information, and medical information. Summit has a HIPAA Privacy Policy.

On October 18, 2024, Summit sent notice letters indicating that, in April, it had discovered suspicious activity on its computers. The details regarding this information and the individual Plaintiffs experiences are discussed below in the Analysis section.

On October 23, 2024, this first lawsuit was filed (D. 1). The Court ordered consolidation of the nine purported class actions related to the data breach into this case (D. 9). Plaintiffs filed a consolidated Complaint (D. 13). Plaintiffs bring nine claims: (1) negligence; (2) negligence per se; (3) breach of implied contract; (4) breach of fiduciary duty; (5) intrusion upon seclusion / public disclosure of private facts; (6) unjust enrichment; (7) violation of Colorado Consumer Protection Act (CCPA), Colo. Rev. Stat. §§ 6-1-105(1); (8) violation of Colorado Security Breach Notification Act, Colo. Rev. Stat. §§ 6-1-716; and (9) for declaratory judgment (D. 13). Defendant seeks dismissal of all claims (D. 29). After briefing was complete, Plaintiff's filed a Notice of Supplemental Authority (D. 32) and a corrected opposition (D. 52-1). On March 3, 2026, the Court held a hearing on the motion (D. 53).

II. LEGAL STANDARD

A. Federal Rule of Civil Procedure 12(b)(1) and Standing

Federal courts are courts of limited jurisdiction and have an independent obligation to determine whether subject matter jurisdiction exists at any stage of the litigation. *Image Software, Inc. v. Reynolds & Reynolds Co.*, 459 F.3d 1044, 1048 (10th Cir. 2006). "Federal jurisdiction is

determined based on the facts as they existed at the time the complaint was filed." *Id*. (citing *Smith v. Sperling*, 354 U.S. 91, 93 n. 1 (1957)); 28 U.S.C. § 1332.

Under Rule 12(b)(1), a party may seek dismissal for lack of subject matter jurisdiction in two forms: (1) facial attack or (2) factual challenge. For the first, the moving party may "facially attack the complaint's allegations as to the existence of subject matter jurisdiction." *Merrill Lynch Bus. Fin. Servs., Inc. v. Nudell*, 363 F.3d 1072, 1074 (10th Cir. 2004). When reviewing a facial attack, courts accept a complaint's allegations in the complaint as true. *See Pueblo of Jemez v. United States*, 790 F.3d 1143, 1148 n.4 (10th Cir. 2015) (citation omitted). For the second, a party may go beyond the complaint's allegations by presenting evidence challenging the factual basis "upon which subject matter jurisdiction rests." *Nudell*, 363 F.3d at 1074 (citation omitted). When reviewing a factual challenge, courts cannot "presume the truthfulness of the complaint's factual allegations," and may consider documents outside the complaint without converting the motion to dismiss into a motion for summary judgment. *Pueblo of Jemez*, 790 F.3d at 1148 n.4. The party invoking jurisdiction bears the burden of establishing subject matter jurisdiction. *Basso v. Utah Power & Light Co.*, 495 F.2d 906, 909 (10th Cir. 1974).

Under Article III of the United States Constitution, federal courts only have jurisdiction to hear certain "cases" and "controversies." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157 (2014). "[A] court must raise the standing issue sua sponte, if necessary, in order to determine if it has jurisdiction." *United States v. Colorado Supreme Ct.*, 87 F.3d 1161, 1166 (10th Cir. 1996). "A federal court is powerless to create its own jurisdiction by embellishing otherwise deficient allegations of standing." *Nova Health Sys. v. Gandy*, 416 F.3d 1149, 1154 (10th Cir. 2005). Standing jurisprudence has two categories: (1) Article III (which enforces the case or controversy

requirement of the United States Constitution) and (2) prudential (judicially self-imposed limits on the exercise of federal jurisdiction"). *Wilderness Soc'y. v. Kane Cnty*., 632 F.3d 1162, 1168 (10th Cir. 2011) (quotation marks omitted).

Standing under Article III is a threshold issue that must be addressed before the putative plaintiff can litigate their claims in federal court. *Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 475–76 (1982). To establish Article III standing, a plaintiff must allege that:

> (1) it has suffered an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000); *see also TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021). A plaintiff bears the burden of establishing standing. *Colorado Outfitters Ass'n v. Hickenlooper*, 823 F.3d 537, 544 (10th Cir. 2016).

B. Federal Rule of Civil Procedure 12(b)(6)

Under Rule 12(b)(6), a court may dismiss a complaint for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true and interpreted in the light most favorable to the non-moving party, to state a claim to relief that is plausible on its face. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Additionally, the complaint must sufficiently allege facts supporting all the elements necessary to establish an entitlement to relief under the legal theory proposed; however, a complaint may be dismissed

because it asserts a legal theory not cognizable as a matter of law. *Forest Guardians v. Forsgren*, 478 F.3d 1149, 1160 (10th Cir. 2007); *Golan v. Ashcroft*, 310 F. Supp. 2d 1215, 1217 (D. Colo. 2004). A claim is not plausible on its face "if [the allegations] are so general that they encompass a wide swath of conduct, much of it innocent," and the plaintiff has failed to "nudge[the] claims across the line from conceivable to plausible." *Robbins v. Oklahoma*, 519 F.3d 1242, 1247 (10th Cir. 2008) (quoting *Twombly*, 550 U.S. at 570). In assessing a claim's plausibility, legal conclusions contained in the complaint are not entitled to the assumption of truth. *See Kansas Penn Gaming, LLC v. Collins*, 656 F.3d 1210, 1214 (10th Cir. 2011). The standard, however, remains a liberal pleading standard, and "a well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable, and that a recovery is very remote and unlikely." *Dias v. City & Cty. of Denver*, 567 F.3d 1169, 1178 (10th Cir. 2009) (internal quotations and citation omitted).

III. ANALYSIS

There are two broad issues for the Court to resolve: standing and whether the claims have been sufficiently pled.

A. Plaintiffs Have Alleged Standing.

For applying the three-element test for standing in the context of a data breach, the Court finds the framework applied in *In re Progressive Leasing Breach Litig.*, No. 2:23-CV-00783-DBB-CMR, 2025 WL 213744 (D. Utah Jan. 16, 2025), to be persuasive and instructive. After a thorough review of the caselaw, Judge David Barlow explained:

> first, misuse is generally necessary to obtain standing; second, at the pleadings stage, allegations of misuse by some plaintiffs often can suffice to plausibly show that other plaintiffs' injury is imminent. Once the injury is deemed imminent, plaintiffs can potentially allege

> a concrete injury based on lost money and time spent on mitigating the imminent harm, and perhaps the emotional distress occasioned by the imminent misuse. With these conclusions in mind, the court turns to Plaintiffs' allegations.

(*id*. at *9).

Applying this framework here shows that Plaintiffs have sufficiently alleged standing.[2] There are allegations of misuse by some plaintiffs that are plausibly tied to the broad swath of data potentially subject to the data breach tied to allegations of time spent mitigating those impacts. Plaintiffs' allegations in the Complaint that there was an increase in targeted spam calls and other communications to the phone numbers and other contact information held by defendants that caused harm of lost time and emotional injury are sufficient at this stage. Plaintiffs allege harms that arise out of a data breach including related demands on their time, both to mitigate in the event that their data was stolen and as a result of attendant fraud, etc. The allegedly stolen data here is alleged to include extensive personal information and contact information. Thus, efforts to protect personal data and time lost to increased spam and the like each represent concrete injuries. Accordingly, the Court finds that Plaintiffs have Article III standing.

Defendant's arguments that standing is lacking and the allegations in the complaint are insufficient largely boil down to an assertion that all that is alleged here is a mere breach without attendant ill effects on Plaintiffs (*e.g.*, D. 29 at 13) ("Plaintiffs cannot establish an injury in-fact by alleging future risk of harm"). These arguments mostly depend on reference to Defendant's breach notification, which asserts that each Plaintiffs' data "may have been accessed" and that "there is no evidence that [their] information has been misused" (*see id*. at 10). But the Court must look to

[2] Defendant does not challenge any Plaintiff individually.

the factual allegations in the complaint and accept them as true. And the Complaint sufficiently alleges facts tying the alleged breach to Plaintiff's harms, particularly by linking the types of information stored by Defendants and exfiltrated in the breach to harms that it is reasonable to infer, based on temporal relationship and other facts, are connected to the breach. By way of example, Plaintiffs allege that, after the breach, "Plaintiff Smith began receiving an excessive number of spam robocalls and text (20-30 per day) on the same cell phone number that Plaintiff Smith provided to Summit" and "was a victim of attempted fraud" at his bank "July or August of 2024" (D. 13 at 35–36). Similarly, "Plaintiff Richardson began receiving an excessive number of spam calls on the same cell phone number that Plaintiff Richardson provided to Summit experienced an increase in phishing emails, up to approximately 150 a day *related to medical issues*" (*id*. at 38) (emphasis added). Alarmed by this and the breach, "Richardson purchased credit monitoring services and services to delete his information from the dark web costing over $300" (*id*. at 39). It is reasonable to infer both misuse of exfiltrated data and harms to Plaintiffs caused by that misuse. This is sufficient for standing. *In re Progressive Leasing Breach Litig.*, 2025 WL 213744, at *9.

Defendant also seeks to strike the class allegations on the basis of a failure to plead standing (D. 29 at 31). Having found that Plaintiffs have sufficiently pled standing, the Court declines to strike the class allegations at this point. Whether the class is properly structured to encompass members that have standing is better addressed through the class certification process and with the benefit of some discovery. *Hudson v. HomeAdvisor, Inc.*, 348 F.R.D. 690, 693 (D. Colo. 2025). The concerns raised by Defendant "do not justify the drastic measure of striking the class

allegations in their entirety." *Manning v. Bos. Med. Ctr. Corp.*, 725 F.3d 34, 60 (1st Cir. 2013). Accordingly, the Court will not dismiss for lack of jurisdiction or strike the class allegations.

B. Plaintiffs State Some Claims but Others Fail.

1. Plaintiffs State a Negligence Claim.

"To establish a prima facie case of negligence, a plaintiff must demonstrate the following elements: '(1) the existence of a legal duty to the plaintiff; (2) the defendant breached that duty; (3) the plaintiff was injured; and (4) the defendant's breach of duty caused the injury.'" *Dolin v. Contemp. Fin. Sols., Inc.*, 622 F. Supp. 2d 1077, 1082 (D. Colo. 2009) (quoting *Raleigh v. Performance Plumbing and Heating, Inc.*, 130 P.3d 1011, 1015 (Colo. 2006)).

Defendant argues that the negligence claim fails because it did not owe a duty of care to Plaintiffs because harm was not foreseeable and because Plaintiffs have not alleged actual damages (D. 29 at 22–25).

i. Harm to Plaintiffs was Foreseeable.

Plaintiffs argue that "by collecting and storing Plaintiffs' Private Information in its computer property, as well as sharing that information and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard the information from theft and unauthorized disclosure" (D. 52-1 at 24). They assert that this duty can be judged against "industry standards" as well as statutes requiring protective measures (*id.*). Although Defendant argues that it was not aware of a specific threat against it, so no harm was foreseeable (D. 29 at 23),[3] Plaintiffs note their factual allegations indicating that it is "well-known that Private Information, particularly

[3] Defendant's argument is difficult to square with the alleged facts, which involve a significant delay between Defendant's discovery on "April 18, 2024," of "suspicious activity within [its] computer environment" and the notification months later (D. 13-1 at 7). Even assuming Defendant did not know of a specific threat before, it did after discovering the suspicious activity.

Social Security numbers, is a valuable commodity and a frequent, intentional target of cybercriminals, particularly within the healthcare industry" (D. 30 at 24).

The Court agrees that Plaintiffs have sufficiently alleged foreseeability. In addition to the factual allegations in the complaint (*see* D. 13 at ¶¶ 50–63, 68–78), the statutes identified by Plaintiff reflect a well-established understanding that it is foreseeable that cybercriminals will target healthcare providers. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires the adoption of extensive security safeguards for patient information including through compartmentalization of information and technical safeguards. 42 U.S.C. § 1320d-2(d). Such security standards for health information serve the explicit purpose to "protect against any reasonably anticipated—(i)threats or hazards to the security or integrity of the information; and (ii)unauthorized uses or disclosures of the information." *Id*. § 1320d-2(d)(2)(B).

In view of the foreseeability of harm, a duty by health care providers to ensure that patient data they acquire and store is protected fits within the framework used to judge whether such a duty exists under Colorado law. "In determining whether a duty should be recognized, a court must consider many factors, including: (1) the risk involved, (2) the foreseeability and likelihood of injury as weighed against the social utility of the actor's conduct, (3) the magnitude of the burden guarding against injury or harm, and (4) the consequences of placing the burden upon the actor." *HealthONE v. Rodriguez ex rel. Rodriguez*, 50 P.3d 879, 888 (Colo. 2002) (citations omitted). The well-pleaded factual allegations indicate a significant risk to patients, that injury is foreseeable in the absence of protection due to pervasive cybersecurity risk. Even in reply, Defendant does not assert any particular burden or attendant consequences that would attend such

a duty (*see* D. 31 at 20).[4] Accordingly, the Court rejects Defendant's argument that they did not owe a duty because harm was not foreseeable.

ii. Plaintiffs Have Alleged Damages.

Defendant's damages argument is a rehash of its standing argument discussed above (D. 29 at 24) ("As further explained in the Article III standing analysis above"). The Court rejects this argument for the same reasons discussed above. Accordingly, the Court denies dismissal of Plaintiffs' negligence claim.

2. Negligence Per Se.

"Negligence per se occurs when a defendant violates a statute adopted for the public's safety and the violation proximately causes a plaintiff's injury." *Miller v. Crested Butte, LLC*, 2024 CO 30, ¶ 27, 549 P.3d 228, 234 (citing *Scott v. Matlack, Inc.*, 39 P.3d 1160, 1166 (Colo. 2002)). "To prevail on a negligence per se claim, a plaintiff 'must also demonstrate that the statute was intended to protect against the type of injury she suffered and that she is a member of the group of persons the statute was intended to protect.'" *Id*. (quoting same).

The Parties present conflicting views of the law with regard to whether Plaintiff can bring a negligence per se claim based on HIPAA and the Gramm-Leach-Bliley Act (FTC Act), but none cites binding authority resolving this question. The Court is persuaded by the reasoning of *Owen-Brooks* that a negligence per se claim based on HIPAA and the FTC Act is viable under Colorado law because "Colorado law has recognized that a statute may provide evidence of the standard of

[4] Given the lack of briefing on this issue, the Court declines to determine the existence and scope of the relevant duty at this point. *See HealthONE*, 50 P.3d at 888; *Owen-Brooks v. DISH Network Corp*., No. 1:23-CV-01168-RMR-SBP, 2024 WL 4333660, at *2 (D. Colo. Sept. 27, 2024) ("This Court agrees with Magistrate Judge Prose—additional information is needed to determine whether a legal duty exists."). Defendant's argument is focused on an assertion that the alleged harm was not foreseeable, and the Court finds that it was on the facts alleged and in view of the

care for a negligence per se claim even if the statute does not allow for a private right of action." *Owen-Brooks*, 2024 WL 4333660, at *2 (citing *Dolin v. Contemp. Fin. Sols., Inc.*, 622 F. Supp. 2d 1077, 1085 (D. Colo. 2009)); *see also Charlie v. Rehoboth McKinley Christian Health Care Servs.*, 598 F. Supp. 3d 1145, 1159 (D.N.M. 2022) (allowing negligence per se claim to proceed and distinguishing contrary cases). As discussed above, HIPAA requires the creation of regulations setting out security standards for the protection of patient data. The FTC Act similarly has been used as a basis to set minimal requirements for those dealing with consumer data through the Standards for Safeguarding Customer Information (Safeguards Rule). 16 C.F.R. 314.1(a) ("This part . . . sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.").

Plaintiffs here sufficiently allege that they fall within the groups intended to be protected by these statutes, namely, patients sharing data with healthcare providers and consumers providing data to institutions over which the FTC has jurisdiction.[5] The requirement that a negligence per se claim must be based on a "statute adopted for the public's safety" is not a bar to Plaintiff's claim. *Bullock v. Wayne*, 623 F. Supp. 2d 1247, 1252 (D. Colo. 2009), *as amended* (Apr. 17, 2009). Although the standards under HIPAA and the Safeguards Rule are directed at data, the unambiguous intent is to protect the safety of the patients and consumers themselves. *Integrity Applied Sci., Inc. v. Clearpoint Chemicals LLC*, No. 1:18-CV-02235-DDD-NYW, 2020 WL 12584444, at *3 (D. Colo. Apr. 20, 2020) (reasoning that a Colorado statute criminalizing

[5] The Safeguards Rule applies to broadly defined "'financial institutions' over which the Commission has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act." 16 C.F.R. 314.1(b). Assuming the truth of Plaintiffs' allegations, it is plausible to infer that Defendant falls within this broad definition.

cybercrime was adopted for public safety). Accordingly, the Court denies dismissal of Plaintiffs' negligence per se claim.

3. Defendant's Breach of Fiduciary Duty Argument Depends on its Rejected Negligence Argument.

"In order to recover on a claim for breach of fiduciary duty, a plaintiff must prove: 1) that the defendant was acting as a fiduciary of the plaintiff; 2) that he breached a fiduciary duty to the plaintiff; 3) that the plaintiff incurred damages; and 4) that the defendant's breach of fiduciary duty was a cause of the plaintiff's damages. *Graphic Directions, Inc. v. Bush*, 862 P.2d 1020, 1022 (Colo. App. 1993) (citing CJI–Civ.2d 26:1 (1989)).

Defendant asserts that the "breach of fiduciary duty claim must be dismissed for the same reasons their negligence claim fails" (D. 29 at 26). Because the Court rejected that argument above, it also rejects this argument. *Cf. Martinez v. Lewis*, 969 P.2d 213, 220 (Colo. 1998) (holding that an insurance company's doctor owed a fiduciary duty to customer he examined even in absence of physician-patient relationship); *Charlie*, 598 F. Supp. 3d at 1160 (rejecting the argument that a hospital's fiduciary duty did not include care for patient information). Accordingly, the Court denies dismissal of Plaintiffs' breach of fiduciary duty claim.

4. Breach of Implied Contract.

A breach of contract claims has four elements: "(1) the existence of a contract, (2) performance by the plaintiff or some justification for nonperformance, (3) failure to perform the contract by the defendant, and (4) resulting damages to the plaintiff." *W. Distrib. Co. v. Diodosio*, 841 P.2d 1053, 1058 (Colo. 1992). Liability exists "only if" a plaintiff can show "all the elements of the formation and breach of a contract." *Tuttle v. ANR Freight Sys., Inc.*, 797 P.2d 825, 827 (Colo. App. 1990) (citing *Continental Air Lines, Inc. v. Keenan*, 731 P.2d 708 (Colo. 1987)).

"Implied in fact contracts arise from conduct of the parties which evidences a mutual intention to contract with each other." *Id*. at 829 (citing *A.R.A. Manufacturing Co. v. Cohen*, 654 P.2d 857 (Colo. App. 1982)).

Plaintiffs rely on their allegations that they "transmitted monies directly and/or indirectly to Defendant for services with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security" and that Defendant had a HIPAA policy expressing it was "committed" to protecting the privacy of patient information to assert that there was an implied contract (D. 13 at ¶¶ 37, 256). Although it is a close question, the Court concludes that Plaintiffs have failed to allege the formation of an implied contract with Defendant. Colorado courts have recognized that statements of commitment can imply contractual obligation, but the terms of that commitment must be sufficiently specific to allow the formation of a contract. *Tuttle*, 797 P.2d at 828 (distinguishing cases rejecting an implied contract on the basis its commitment was "more detailed"). Here, the alleged terms of the contract are wholly unclear. The alleged HIPAA policy expresses nothing more than a generic commitment to "protecting the privacy of your protected health information" and a notification that relevant laws exist (D. 13 at ¶ 37). Accordingly, the Court dismisses Plaintiffs' breach of implied contract claim.

5. Plaintiff Has Not Stated Invasion of Privacy Claims.

i. Defendant is not Alleged to Have Intruded on Plaintiffs' Seclusion.

A claim for intrusion on seclusion is "intentional tort in which a plaintiff must establish that: (1) another person has intentionally intruded, physically or otherwise; (2) upon the plaintiff's seclusion or solitude; and (3) such intrusion would be offensive or objectionable to a reasonable person." *Doe v. High-Tech Inst., Inc.*, 972 P.2d 1060, 1067 (Colo. App. 1998), *as modified on*

denial of reh'g (Aug. 6, 1998); *see also* Restatement (Second) of Torts § 652B (1981) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

Plaintiffs argue that that "sufficiently allege intent, by virtue of their allegations that Defendant intentionally cut corners to save costs on data security" (D. 52-1 at 29). This is insufficient because intentionally cutting corners is not itself an intrusion. *High-Tech Inst., Inc.*, 972 P.2d at 1068-69 (noting that, although there is a privacy interest in medical information, the voluntary collection of that information is not an intrusion on seclusion); *see also Slaughter v. John Elway Dodge Sw./AutoNation*, 107 P.3d 1165, 1171 (Colo. App. 2005) ("The tort of invasion of privacy by intrusion 'requires an unreasonable manner of intrusion or an intrusion for an unwarranted purpose.'" (quoting *Denver Publ'g Co. v. Bueno*, 54 P.3d 893 (Colo. 2002))). Accordingly, the Court dismisses Plaintiffs' intrusion on seclusion claim.

ii. Plaintiff has not Alleged Public Disclosure.

Colorado recognizes "a tort claim for invasion of privacy in the nature of unreasonable publicity given to one's private life" requiring that "(1) the fact or facts disclosed must be private in nature; (2) the disclosure must be made to the public; (3) the disclosure must be one which would be highly offensive to a reasonable person; (4) the fact or facts disclosed cannot be of legitimate concern to the public; and (5) the defendant acted with reckless disregard of the private nature of the fact or facts disclosed." *Robert C. Ozer, P.C. v. Borquez*, 940 P.2d 371, 377 (Colo. 1997). "The requirement of public disclosure connotes publicity, which requires communication

to the public in general or to a large number of persons, as distinguished from one individual or a few." *Id*. (citing *Brown v. Mullarkey*, 632 S.W.2d 507, 509–10 (Mo. Ct. App. 1982)).

Plaintiff asserts that it meets the publicity requirement with its allegations that because "their Private Information was disclosed to cybercriminals and then disseminated on the Dark Web" (D. 52-1 at 29). The factual allegations in the complaint, however, do not support a conclusion that Plaintiff's information was made public. Rather, Plaintiff's allege that the data is available for sale on the dark web and that cybercriminals offer such information for sale (D. 13 at 3, 17). Obviously, publicly posting the information would destroy any sale value. Accordingly, the Court dismisses Plaintiffs' public disclosure of private facts claim.

6. Defendant's Unjust Enrichment Argument is Predicated on its Rejected Standing Argument.

Defendant's argument for dismissal of the unjust enrichment is a restatement of its standing argument discussed above (D. 29 at 29) ("as explained in the Article III standing analysis above, Plaintiffs received exactly what they bargained for, medial services"). The Court rejects this argument for the same reasons discussed above. Accordingly, the Court denies dismissal of Plaintiffs' unjust enrichment claim.

7. The CCPA Has Been Amended to Allow Class Actions.

In its motion, Defendant seeks dismissal of the CCPA claim on the basis that recovery is not available in a class action (D. 29 at 30 ("As the CCPA expressly excludes liability in a putative class action, Plaintiffs' CCPA claim must be dismissed."). Plaintiffs respond that recent amendments allow recovery by class action (D. 52-1 at 31) (citing Colo. Rev. Stat. § 6-1-113(2.9); *An Act Concerning Available Relief For Plaintiffs Who Prevail In A Class Action Under The "Colorado Consumer Protection Act"*, CO LEGIS 36 (2022), 2022 Colo. Legis. Serv. Ch. 36

(H.B. 22-1071)). In reply, Defendant does not dispute the effect of the amendment and, instead, raises new arguments not found in its motion (D. 34 at 23–24). The Court declines to address these untimely arguments and denies dismissal of the CCPA claim.

8. The Colorado Security Breach Notification Act May Allow Private Claims.

Defendant argues that the Colorado Security Breach Notification Act does not allow for private lawsuits (D. 52-1 at 31). While the Act does not expressly provide for private actions, in allowing for actions by the attorney general it explicitly provides that "provisions of this section are not exclusive." Colo. Rev. Stat. § 6–1–716(4). Courts that have addressed this issue on the merits have declined to dismiss such claims at the pleadings phase due to the ambiguity of the statue. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014) ("This permissive language is, as Plaintiffs' argue, at least ambiguous as to whether there is a private right of action under Colorado law."); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1341 (N.D. Ga. 2019) ("The Defendants have not identified any authority construing this language as precluding private rights of action. Absent such authority, the Court declines to dismiss the Plaintiffs' claims under the Colorado" breach statute). The Court finds this authority persuasive and declines to dismiss this claim at this point.

9. Defendant's Declaratory Judgment and Injunctive Relief Argument is Based on its Rejected Standing Argument.

Defendant's argument for dismissal of the "claims" for declaratory and injunctive relief is a restatement of its standing argument discussed above (D. 29 at 31) ("as Plaintiffs lack Article III standing, and their Declaratory Judgment Act claim is duplicative of the relief sought in their other claims"). The Court rejects this argument for the same reasons discussed above. Accordingly, dismissal of these requests for relief are denied.

IV. CONCLUSION

Accordingly, Defendant's Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint and Motion to Strike Class Allegations (D. 29) is GRANTED IN PART and DENIED IN PART as set forth above. It is FURTHER ORDERED that Claim Five is dismissed.

DATED March 9, 2026.

BY THE COURT:

Gordon P. Gallagher
United States District Judge