UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

Darryl Scott v. Healthcare Management Solutions, LLC, et al.

Scott · No. 1:25-CV-12 · Decided March 31, 2026

OPINION

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF WEST VIRGINIA DARRYL SCOTT, Plaintiff, v. Civ. Action No. 1:25-CV-12 (Judge Kleeh) HEALTHCARE MANAGEMENT SOLUTIONS, LLC, et al., Defendants. MEMORANDUM OPINION AND ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTION TO DISMISS [ECF NO. 66] Pending before the Court is the Motion to Dismiss by Defendants AFDS and HMS [ECF No. 66].For the reasons stated herein, Defendants AFDS and HMS's Motion is GRANTED IN PART and DENIED IN PART.

I. PROCEDURAL BACKGROUND Named Plaintiff, Darryl Scott ("Scott"), first filed the Class Action Complaint in the Northern District of California on August 1, 2024. ECF No. 1. Defendants Healthcare Management Solutions, LLC, ("HMS") and ASRC Federal Data Solutions, LLC ("ASRC", collectively "Defendants") filed their Motion to Dismiss, or Alternatively to Transfer Venue on October 15, 2024.

ECF No. 20. Scott filed his Amended Complaint on November 4, 2024. ECF No. 23. Defendants filed their Motion to Dismiss for Lack of Jurisdiction in the Northern District of California on December 3, 2024. ECF No. 34.

The motion included arguments under Rule 12(b)(1), Rule 12(b)(2), and Rule 12(b)(3) of the Federal Rules of Civil Procedure. Id. Defendants' motion alternatively requested the case be transferred pursuant to Rule 12(b)(4) of the Federal Rules of Civil Procedure. Id. Defendants' alternative motion to transfer venue was granted by the Northern District of California on February 7, 2025.

ECF No. 41. The case was transferred to this Court. Scott did not file a Second Amended Complaint, Defendants filed a Motion to Dismiss on April 11, 2025. ECF No. 66. Defendants' motion argues for dismissal pursuant to Rule 12(b)(1) and Rule 12(b)(6) of the Federal Rules of Civil Procedure. Id. Scott's response in opposition of Defendants' Motion to Dismiss was filed on May 12, 2025.

ECF No. 73. Defendants' reply in support of their motion was filed on June 2, 2025. ECF No. 77. The Court heard oral argument on the subject motion on October 20, 2025. On November 17,

2025, Defendants filed Defendants' Notice of Supplemental Authority in Support of Motion to Dismiss [ECF No. 95], which Plaintiff responded to on November 24, 2025 [ECF No. 96].

II. FACTUAL BACKGROUND This case stems from a ransomware attack on HMS, a private entity subcontracted by ASRC, to manage personal data for Medicare beneficiaries that resulted in a data breach allegedly affecting over 250,000 individuals. ECF No. 23 at ¶¶ 1, 7. Named Plaintiff, Darryl Scott, alleges he suffered extensive injuries, including identify theft and fraud, resulting from this data breach.

Id. at ¶ 8,9. Specifically, Plaintiff Scott alleges he has been targeted by pervasive and ongoing identity theft crimes, including fraudulent short-term loans that were made using personal information compromised by the data breach. Id. at ¶¶ 11, 76.

The Amended Complaint alleges that Scott and proposed class members were required to provide sensitive PHI and PII to CMS as a prerequisite to obtaining Medicare benefits. Id. at ¶ 26. HMS learned as early as October 2022, that its network suffered from a data breach and ransomware attack, which exposed the PII and PHI of Scott and other Medicare beneficiaries, including: • Full name of the beneficiary • Address • Date of Birth • Phone Number • Full Social Security Number • Medicare Beneficiary Identifier • Banking Information, including routing and account numbers • Medicare Entitlement, Enrollment, and Premium Information.

Id. at ¶¶ 32-33. Medicare beneficiaries learned of the data breach in December 2022. Id. at ¶ 34. Scott alleges that because of the data breach, he was forced to take measures to mitigate the harm, including spending time monitoring credit and financial accounts, researching the data breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft.

Id. at ¶ 75. Scott further alleges he has suffered extensive actual injuries and has been repeatedly victimized by identity theft and fraud associated with the breached data, including fraudulent bank accounts, loans, and payments under his name. Id. at ¶ 76. Further, Scott asserts he experienced decreases to his credit score, reductions in his ability to access his bank account, and serious difficulties taking out legitimate loans because of the data breach.

Id. at ¶ 78. Scott filed his Amended Class Action Complaint on November 4, 2024, alleging the following causes of action: Count I: Negligence Count II: Breach of Implied Contract Count III: Breach of Fiduciary Duty Count IV: Invasion of Privacy Count V: Cal. Civ. Code § 1798.80 et seq.; California Customer Records Act Count VI: Cal. Bus. & Prof. Code §§ 17200, § 17200 et seq.; California Unfair Competition Law Count VII: Cal. Civ.

Code § 56.10 et seq.; California Confidentiality Medical Information Act Count VIII: 28 U.S.C. § 2201 et seq.; Declaratory Relief. ECF No. 23. III. LEGAL STANDARD Rule 12(b)(1) Rule 12(b)(1) of the Federal Rules of Civil Procedure allows the Court to dismiss an action for lack of

jurisdiction over the subject matter. A plaintiff bears “the burden of proving that subject matter jurisdiction exists.” Evans v. B.F.

Perkins Co., 166 F.3d 642, 647 (4th Cir. 1999) (citation omitted). In considering a motion to dismiss pursuant to Rule 12(b)(1), the court should “regard the pleadings as mere evidence on the issue, and may consider evidence outside the pleadings without converting the proceeding to one for summary judgment.” Id. (citation omitted).

The court should grant the motion “only if the material jurisdictional facts are not in dispute and the moving party is entitled to prevail as a matter of law.” Id. (citation omitted). When a defendant asserts multiple defenses, “questions of subject matter jurisdiction must be decided first, because they concern the court's very power to hear the case.” Owens-Illinois, Inc. v. Meade, 186 F.3d 435, 442 n.4 (4th Cir.

1999) (citations and internal quotation marks omitted). Rule 12(b)(6) Rule 12(b)(6) of the Federal Rules of Civil Procedure allows a defendant to move for dismissal upon the ground that a Complaint does not “state a claim upon which relief can be granted.” In ruling on a motion to dismiss, a court “must accept as true all of the factual allegations contained in the Complaint.” Anderson v. Sara Lee Corp., 508 F.3d 181, 188 (4th Cir.

2007) (quoting Erickson v. Pardus, 551 U.S. 89, 94 (2007)). A court is “not bound to accept as true a legal conclusion couched as a factual allegation.” Papasan v. Allain, 478 U.S. 265, 286 (1986). A motion to dismiss under Rule 12(6)(b) tests the “legal sufficiency of a Complaint.” Francis v. Giacomelli, 588 F.3d 186, 192 (4th Cir. 2009). A court should dismiss a Complaint if it does not contain “enough facts to state a claim to relief that is plausible on its face.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 570 (2007).

Plausibility exists “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).

The factual allegations “must be enough to raise a right to relief above a speculative level.” Twombly, 550 U.S. at 545. The facts must constitute more than “a formulaic recitation of the elements of a cause of action.” Id. at 555. A motion to dismiss “does not resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses.” Republican Party of N.C. v. Martin, 980 F.2d 942, 952 (4th Cir.

1992). IV. DISCUSSION Defendants move to dismiss Plaintiff’s Complaint pursuant to Rule 12(b)(1) and Rule 12(b)(6) of the Federal Rules of Civil Procedure for lack of subject matter jurisdiction and failure to state a claim.

In his response, Scott agreed to voluntarily dismiss his breach of fiduciary duty claim (Count Three); therefore, Defendant's motion with respect to Count Three is GRANTED. ECF No. 73 at p. 14 n. 7. The remaining issues before this Court are whether Scott has standing to bring his complaint, and whether Scott alleged facts sufficient to plausibly establish his negligence claim, negligence per se claim, breach of implied contract claim, invasion of privacy claim, California Customer Records Act claim, California Unfair Competition Law claim, California Confidentiality of Medical Information Act claim, and declaratory judgment claim.

For the reasons discussed below, the Court GRANTS IN PART and DENIES IN PART Defendants' Motion to Dismiss [ECF No. 66]. A. Standing The Court DENIES Defendants' motion to dismiss with respect to Rule 12(b)(1) of the Federal Rules of Civil Procedure.

The judicial power vested by Article III of the Constitution extends only to "cases" and "controversies." U.S. Const. art. III, § 2. Because federal courts are courts of limited jurisdiction, a plaintiff must first establish standing to bring suit. See Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).

To establish Article III standing, a plaintiff is required to show the following: (1) an injury in fact (i.e., a concrete and particularized invasion of a legally protected interest); (2) causation (i.e., a fairly traceable connection between the alleged injury in fact and the alleged conduct of the defendant); and (3) redressability (i.e., it is likely and not merely speculative that the plaintiff's injury will be remedied by the relief plaintiff seeks in bringing suit).

Sprint Commc'ns Co., L.P. v. APCC Servs., Inc., 554 U.S. 269, 273– 74 (2008) (citations and internal punctuation omitted). In a putative class action standing is analyzed "based on the allegations of personal injury made by the named plaintiff." Hutton v. Nat'l Bd. 0f Exam'rs in Optometry, Inc., 892 F.3d 613, 620 (4th Cir. 2018) (citation omitted).1 1. Injury-in-fact The Court finds that Scott's alleged injury satisfies the injury-in-fact element of standing. "Standing is not confined to those who can show economic harm." Id. at 622 (citation modified).

Specifically, in data breach cases, a plaintiff may satisfy the injury-in-fact element of standing when he experiences identity theft, fraud, a decrease in credit score, or spends time and resources mitigating a substantial risk of harm. Id. (finding the injury-in-fact element was satisfied where a plaintiff's credit 1 Upon review of Holmes v. Elephant Insurance Co., 156 F.4th 413 (4th Cir.

2025), which Defendants provided as supplemental authority, the Court finds that this case does not further Defendants' position. Rather, as in Holmes where certain Plaintiffs' driver's license numbers were actually posted on the dark web, Scott alleges actual misuse of his PHI and PII because he experienced multiple instances of identity theft and fraud, not just an increased risk. score decreased, she suffered lost time and out-of-pocket expenses mitigating the data breach, and she received unsolicited credit cards taken out in her name).

Defendants contend that Plaintiff's alleged injuries — increased risk of identity theft, increased risk of fraud, and time spent mitigating his personal and financial information — are generic in nature, merely speculative, and not imminent. Scott asserts that the specified, actual instances of identity theft and fraud, his decreased credit score, and the time spent mitigating a substantial risk of identity theft and fraud are particularized and concrete.

Here, Scott satisfies the injury-in-fact element of standing because he alleged a concrete particularized injury. Scott alleges fraudulent bank accounts were created under his name with his information; fraudulent short-term loans associated with his personal information were taken out; unauthorized changes were made to his bank account and credit file; he spent time and money mitigating his injuries associated with the data breach; and his credit score decreased because of the breach.

Importantly, the CMS notice attached to the Amended Complaint confirms that the compromised information is the kind of information required to commit the identity theft and fraud Scott experienced. Even though Scott did not necessarily suffer economic harm, the alleged specific instances of identity theft and fraud, coupled with the time and resources spent monitoring for identity theft and fraud and his decreased credit score are sufficient to satisfy the injury in-fact element of standing.

2. Traceability The Court finds that Scott's alleged injury satisfies the traceability element of standing. An "injury must be fairly traceable to the challenged action." Hutton, 892 F.3d at 623 (citation omitted). However, the traceability element "is not equivalent to a requirement of tort causation." Id. Indeed, at the motion to dismiss stage, "general factual allegations of injury resulting from the defendant's conduct may suffice." Hutton, 892 F.3d at 620.

In data breach cases, a plaintiff need only allege facts sufficient to establish that the defendant "was a plausible source of [his] personal information." Id. (finding the traceability element was satisfied where a group of plaintiffs determined their information was likely stolen from the defendant because it was the only source they had in common). Scott argues that his alleged injuries are traceable to Defendants because he is not aware of any other data breach that could have compromised his information.

Defendants argue that Scott cannot trace his alleged injuries to Defendants because there has been no forensic investigation to corroborate his allegation. Defendants rely on a class action case filed in the District of Maryland based on the same data breach. Burger v. Healthcare Mgmt. Sols., LLC, No. RDB-23-1215, 2024 WL 473435 (D. Md. Feb. 7, 2024). Defendants' reliance on this case is misplaced.

In Burger, the named plaintiff alleged she experienced "unauthorized charges on her credit card and an increase in spam emails and calls" because of the data breach. Id. at *6. Importantly, the

named plaintiff did not allege that her credit card information, phone number, or email was compromised in the data breach. Id. Nor did she allege that she had to pay for the unauthorized charges.

Id. Ultimately, the District Court held that the named plaintiff lacked Article III standing because her injuries were not traceable to the Defendants. Id. Here, however, Scott's alleged injury satisfies the injury- in-fact requirement and, importantly, he alleges, and the CMS notice attached to the Amended Complaint confirms, that the compromised information is the kind of information required to commit the identity theft and fraud Scott experienced.

Defendants' argument is better served on a motion for summary judgement. Indeed, at the motion to dismiss stage, Scott's allegation that he is unaware of any other data breach that would have compromised his information is sufficient to establish that Defendants were a plausible source of his personal information.

Therefore, Scott satisfies the traceability element of standing. 3. Redressability The Court finds that Scott's injury can be properly redressed with a favorable verdict. For a plaintiff to have standing, he must show that his injury "is likely to be redressed by a favorable judicial decision." Hutton, 892 F.3d at 619.

As the Fourth Circuit noted, "in a breach of data case, 'there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely.'" Id. at 621 n.8. Defendants argue that Scott's injury has already been fully redressed because they offered credit monitoring and other mitigation measures after the data breach.

Scott contends that credit monitoring alone is insufficient to make him whole. Here, Scott's alleged injury could be redressed by a favorable judicial decision because credit monitoring is not sufficient to make Scott whole. Scott alleges his credit score decreased, he spent time and resources mitigating his actual harm and the substantial risk of future harm, and he experienced actual instances of identity theft and fraud.

Simple credit monitoring cannot by itself redress these alleged injuries. As the Fourth Circuit notes, there is no reason to believe that money compensation would not make Scott whole. Therefore, Scott satisfies the redressability element of standing, and the Could DENIES Defendants' Rule 12(b)(1) Motion. B. Negligence/Negligence Per Se The Court DENIES Defendants' Motion to Dismiss with respect to Count One.

In California, a plaintiff must establish four elements to state a claim for negligence: "(1) the defendant had a duty, or an 'obligation to conform to a certain standard of conduct for the protection of others against unreasonable risks,' (2) the defendant breached that duty, (3) that breach proximately caused the plaintiff's injuries, and (4) damages." In re Accellion, Inc. Data Breach Litig., 713 F. Supp. 3d 623, 631 (N.D.

Cal. 2024). Defendants principally argue that they did not owe a duty to Scott; that there was no breach of duty; and, regardless, Scott's negligence claim is barred by the economic loss doctrine. Scott argues that a special relationship existed between Defendants and Scott, which created a duty to protect, that Defendants breached by failing to maintain appropriate and reasonable safeguards to protect Scott's information.

Further, Plaintiff argues the economic loss doctrine does not apply because the existence of a special relationship is an exception to the economic loss doctrine. Alternatively, Scott contends that the economic loss doctrine does not apply because identity theft and decreased credit score are non-economic damages. 2 2 Because there is a special relationship between the parties, Scott's negligence claims are not barred by the economic loss doctrine.

S. Cal. Gas Leak Cases, 441 P.3d 881, 886–87 (Cal. 2019); J'Aire, 598 P.2d at 63. 1. Duty The Court finds that Defendants and Scott had a special relationship; therefore, Defendants owed a duty to Scott. Generally, "each person has a duty to act with reasonable care under the circumstances." Regents of Univ. of Cal. V. Superior Ct. of Los Angeles, 413 P.3d 656, 663 (Cal.

2018). There is "no duty to control the conduct of another, nor warn those endangered by such conduct." Id. at 663–64 (citation omitted). However, there is an exception to this rule in cases where "the defendant has a special relationship... with the victim." Brown v. USA Taekwondo, 483 P.3d 159, 162 (Cal. 2021).

To determine if a duty to protect exists, courts take part in a two-step inquiry. Id. at 161. First, a court determines if a special relationship exists between the parties. Id. Second, if a special relationship exists, a court then determines whether public policy considerations weigh in favor of limiting the duty to protect. Id. a. Special Relationship First, the Court finds that a special relationship exists between Defendants and Scott.

To determine if a special relationship exists between parties, courts look for four common features: (1) that "the relationship has an aspect of dependency in which one party relies to some degree on the other for protection"; (2) where "one party is dependent, the other has superior control over the means of protection"; (3) the relationship is extended "to a limited community, not the public at large"; and (4) the relationship is beneficial to the party with superior control.

Regents, 413 P.3d at 664–65; see also In re Accellion Data Breach Litig., 713 F. Supp. 3d at 632–33 (finding a special relationship existed in a data breach case between data transfer company and effected individuals that used its file transfer system).

Here, all four features are present between Defendants and Scott. Defendants were contracted by CMS to maintain Scott's, and other individuals', PII and PHI. Scott and other Medicare beneficiaries were dependent on Defendants to safeguard their information. Indeed, these beneficiaries had to trust Defendants with their information to receive their Medicare benefits.

Not only were Scott and other Medicare beneficiaries' dependent on Defendants to protect their information, but Defendants also had superior control over the protection of their information. Further, Defendants were not responsible for the public at large; their relationship and responsibility are limited to Medicare beneficiaries.

Finally, Defendants benefitted from their relationship with Scott and other Medicare beneficiaries because Defendants' entire business model is based on maintaining and protecting their PHI and PII. In re Accellion Data Breach Litig., 713 F. Supp. 3d at 633 (finding the fourth feature present where a data transfer's "entire business model was built on promising that it provided a platform to securely transfer files that contained sensitive data").

Defendants argue that no special relationship exists because they were not in a direct relationship with Scott or the other Medicare beneficiaries. But, privity of contract or a direct relationship is not required for a special relationship to exist.

In re Accellion Data Breach Litig., 713 F. Supp. 3d at 634 (explaining that California law does not require "direct correspondence" between parties to find a special relationship exists). Because all four features of a special relationship are present here, a special relationship existed between the parties. b. Policy Considerations Second, the Court finds there are no policy considerations that weigh in favor of limiting Defendants' duty.

To determine if public policy weighs in favor of limiting a duty to protect, courts consider seven factors: (1) "the foreseeability of harm to the plaintiff"; (2) "the degree of certainty that the plaintiff suffered injury"; (3) "the closeness of the connection between the defendant's conduct and the injury suffered"; (4) "the moral blame attached to the defendant's conduct"; (5) "the policy of preventing future harm"; (6) the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach"; and (7) "the availability, cost, and prevalence of insurance for the risk involved." Rowland v. Christian, 443 P.2d 561, 564 (Cal.

1968), superseded by statute on other grounds, Cal. Civ. Code § 847, as stated in Calvillo- Silva v. Home Grocery, Cal., 968 P.2d 65 (Cal. 1998); see also In re Accellion Data Breach Litig., 713 F. Supp. 3d at 635–36 (finding the weight of the Rowland factors in the data protection case did not warrant limiting the defendant's duty to protect). Defendants concede the foreseeability factor but argue that (1) Scott's alleged injuries are speculative; (2) Scott does not allege facts sufficient to connect his alleged harms to Defendants; (3) there is no moral blame because Defendants were merely fulfilling contractual obligations with CMS; and (4) liability would not further any public policies.

None of the points advanced by Defendants are persuasive. Here, the Rowland factors weigh against limiting Defendants' duty to protect Scott and other similarly situated individuals.

Defendants are responsible for maintaining and processing Medicare beneficiaries' PII and PHI for eligibility, entitlement, and premium purposes. This information includes social security numbers, addresses, dates of birth, and other identifying information.

The Medicare beneficiaries are wholly reliant on Defendants to process and protect their data. As stated above, Scott alleged injuries that are concrete, particularized, and traceable to Defendants; therefore, factors two and three weigh against limiting Defendants' duty. Factors four, five, and six weigh against limiting Defendants' duty because, to hold otherwise would create a perverse incentive for companies to turn a blind eye to cyber threats.

Bass v. Facebook, Inc., 394 F.Supp.3d 1024, 1039 (N.D. Cal. 2019) (citing In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1325 (N.D. Ga. 2019)) (holding that the Rowland factors weighed against limiting Facebook's liability); see also In re Accellion Data Breach Litig., 713 F. Supp. 3d at 635–36. Defendants argue that the Court should analyze the existence of a special relationship under the J'Aire factors instead of the four features outlined in Regents.

ECF No. 77 at pp. 7–8. These factors closely track the Rowland factors. Compare Rowland, 443 P.2d at 564, and J'Aire Corp. v. Gregory, 598 P.2d 60, 62–63 (Cal. 1979) ("[T]he court looks at six factors to determine the existence of a special relationship: (1) the extent to which the transaction was intended to affect the plaintiff; (2) the foreseeability of harm to the plaintiff; (3) the degree of certainty that the plaintiff suffered injury; (4) the closeness of the connection between the defendant's conduct and the injury suffered; (5) the moral blame attached to the defendant's conduct; and (6) the policy of preventing future harm.").

Defendants' reliance on the J'Aire factors is of little consequence because the outcome is the same under the J'Aire factors and the Rowland factors. To the extent Defendants' argument relies on cases like In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d. 942 (S.D. Cal. 2012), and In re Zoom Video Commc'ns Inc. Priv. Litig., 525 F. Supp. 3d 1017 (N.D.

Cal. 2021), to avoid liability, Defendants' argument is unpersuasive. Those cases are factually distinguishable from the instant case. As stated above, the Court finds that a special relationship existed between the parties; that Scott alleged actual cognizable harm in the form of experienced identity theft, fraud, and a decreased credit score; and that Scott plausibly alleged that his injuries are connected to Defendants.

Because a special relationship exists between the parties, the alleged harm is connected to Defendants, and because public policy weighs against limiting Defendants' liability, the Court concludes that Defendants owed a duty to Scott and other similarly situated individuals. 2. Breach The Court concludes that Scott sufficiently pled the element of breach. Scott pled two theories to

establish breach: (1) breach of Defendants' duty to protect Scott's PII and PHI and (2) negligence per se.

First, regarding Scott's first theory to establish breach, Defendants principally argue that Scott did not plausibly establish the element of breach because they did not owe him a duty. As stated above, Defendants owed Scott and other similarly situated individuals a duty to protect their PII and PHI. Regardless, Scott alleged facts sufficient to plausibly allege that Defendants breached their duty.

Specifically, Scott alleges deficiencies in Defendants' conduct such as failure to encrypt sensitive data, failure to monitor for intrusion, and failure to mitigate or adequately address the data breach. Here, because existence of the data breach itself may be sufficient at the pleading stage to plausibly allege a breach of duty, Flores-Mendez v. Zoosk, Inc., No. C 20-04929 WHA, 2021 WL 308543, at *4 (N.D.

Cal. Jan. 30, 2021), where a plaintiff pleads deficiencies in a defendant's security measures, he has sufficiently pleaded the element of breach. In re Accellion Data Breach Litig., 713 F. Supp. 3d at 636–37. Indeed, as the Northern District of California reasoned, "it would be 'unreasonable for defendant[s] to insist that the details [regarding its security measures] be laid out in the initial complaint.'" Id.; Flores- Mendez, 2021 WL 308543, at *4.

The Court thus finds that Scott sufficiently pled the element of breach. Second, regarding Scott's second theory to establish breach, Defendants argue that negligence per se cannot attach where the alleged violated statute does not provide a private right of action. Scott argues that the violated statute need not provide a private right of action to satisfy negligence per se.

The California Evidence Code creates a rebuttable presumption of failure to exercise due care when four elements are met: (1) a person "violated a statute, ordinance, or regulation of a public entity"; (2) the violation proximately caused injury to another person; (3) the injury "resulted from an occurrence of the nature which the statute, ordinance, or regulation was designed to prevent"; and (4) the injured person "was one of the class of persons for whose protection the statute, ordinance, or regulation was adopted." Cal. Evid.

Code § 669. The statute relied upon by the plaintiff need not provide a private right of action. See In re Accellion Data Breach Litig., 713 F. Supp. 3d at 640 (allowing the plaintiff to rely on a violation of HIPAA and the FTC Act to establish duty and breach); In re Ambry Genetics Data Breach Litig., 567 F. Supp. 3d 1130, 1142–43 (C.D. Cal. 2021) (same).

Because California Evidence Code § 669 does not require the violated statute, ordinance, or regulation to provide a private right of action, Scott is not barred from asserting violations of HIPAA and the FTC Act to establish breach. 3. Damages Defendants' argument regarding the sufficiency of Scott's alleged damage largely mirrors their standing argument addressed in Section

A. As stated above, because Scott's damages are cognizable, particularized, and traceable to Defendants, Scott has sufficiently pled damages, and the Court DENIES Defendants motion with respect to Count One.

C. Breach of Implied Contract The Court GRANTS Defendants' Motion to Dismiss with respect to Count Two. To establish the existence of an implied contract under California law, a plaintiff must allege "the same elements necessary to evidence an express contract: mutual assent or offer and acceptance, consideration, legal capacity and lawful subject matter." In re Ambry Genetics Data Breach Litig., 567 F. Supp. 3d at 1144 (quoting Corona v. Sony Pictures Entm't, Inc., 2015 WL 3916744, at *5 (C.D.

Cal. June 15, 2015)). A plaintiff must "demonstrate the elements required to establish an implied-in-fact contract: mutual assent, offer and acceptance, and consideration." Smith v. Sabre Corp., 2017 WL 11678765, at *4 (C.D. Cal. Oct. 23, 2017). Additionally, "[p]rivity between parties is a necessary element of an implied-in-fact contract claim." Benay v. Warner Bros. Ent., 2012 WL 13071728, at *4 (C.D.

Cal. Feb. 14, 2012); Rokos v. Peck, 182 Cal.App.3d 604, 617–18 (1986). "An implied contract requires that both parties agree to its terms and have a 'meeting of the minds,' but the creation of an implied contract can be manifested by conduct rather than words." Castillo v. Seagate Tech., LLC, 2016 WL 9280242, at *8 (N.D. Cal. Sept. 14, 2016). Courts have found an implied contract can exist in a data breach context because the "mandatory receipt of Social Security numbers or other sensitive personal information... impl[ies] the recipient's assent to protect the information sufficiently." In re Ambry Genetics Data Breach Litig., 567 F. Supp. 3d at 1144; In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1176 (D.

Minn. 2014). However, such instances involve direct relationships or transactions between the parties. See Id.; see also Peralta v. Certified Emp. Screening Inc., 2025 WL 1723142, at *6 (C.D. Cal. May 7, 2025) (finding an adequately pled breach of implied contract claim when Plaintiffs were required to give Americhek their PII, who in turn provided the PII to its vendor BackChecked who experienced a data breach, because Plaintiffs provided their PII with the reasonable understanding that Americhek would take adequate measures to protect the information and timely disclose any unauthorized access to or theft of their PII).

Compare In re U.S. Vision Data Breach Litig., 732 F. Supp. 3d 369, 377–78 (D.N.J. 2024) (dismissing claim for breach of implied contract because Plaintiff did not plead facts to establish a relationship with the USV defendants. Rather, it was Nationwide that contracted with the USV Defendants, and that the USV Defendants received Plaintiffs' PII/PHI through Nationwide, after Plaintiffs paid for eyecare services) (applying New Jersey law but using same elements for an implied contract).

Defendants maintain that there is no direct relationship between the parties, and they did not receive benefits, therefore, there is no implied contract. ECF No. 67. Specifically, Defendants contend that the Plaintiff only alleges a relationship with CMS and that Defendants did not receive any benefit from Plaintiff, as CMS's contractor. Id. In contrast, Plaintiff claims he adequately pled a breach of implied contact claim, contending that a direct relationship is not required under California common law and Defendants did receive a benefit because they cannot do business without Plaintiff's information.

ECF No. 73. Here, Plaintiff has failed to state a claim for which relief can be granted because he has not sufficiently alleged privity between the parties. Though the exchange of personal information can imply the promise that such information will be protected, the cases finding an implied contract involve direct relationships. "Unlike the cases on which Plaintiff[] rely where the parties had a direct relationship such as business and customer, employee and employer, patient and hospital, or patron and restaurant — here Plaintiff[] failed to plead any facts from which the Court could find any direct relationship." In re U.S. Vision Data Breach Litig., 732 F. Supp. 3d at 377–78.

Plaintiff provided his information to CMS to receive medical benefits and had no direct interactions with Defendants. Rather, Defendants had business relationships with CMS. See ECF No. 1. Compl. at ¶¶ 4-5 ("ASRC contracted CMS in part to resolve system errors related to Medicare beneficiary entitlement and premium payment records...ASRC subsequently subcontracted some or all of these duties in whole or in part to HMS.").

Compare Peralta 2025 WL 1723142, at *6, where Plaintiffs' breach of implied contract claim survived because they directly sued the entity that they gave their PII, after a vendor to which Americhek gave the PII experienced a data breach, with In re U.S. Vision Data Breach Litig., 732 F. Supp. 3d at 377–78, where plaintiffs' claim was dismissed because they did not have a direct relationship with the defendants.

Rather, plaintiffs provided their PHI to their healthcare provider who then gave the PHI to defendants to store and maintain. Like in In re U.S. Vision Data Breach Litig. where Plaintiffs' PHI was accessed via a security breach of their healthcare provider's contractor, here, Plaintiff has failed to allege the existence of a contract with Defendants. Rather, the implied contract for the reasonable security of the PHI in exchange for the PHI would be with CMS.

Accordingly, the Court GRANTS Defendants' motion to dismiss with respect to Count Two because Plaintiff failed to sufficiently allege privity. D. Invasion of Privacy The Court GRANTs Defendants' Motion to Dismiss with Respect to Count Four because no medical information was compromised in the data breach.

To state a claim for invasion of privacy under the California State Constitution a plaintiff has to establish three elements: (1) the plaintiff "possess[es] a legally protected privacy interest"; (2)the plaintiff had a reasonable expectation of privacy; and (3) "the intrusion is so serious in 'nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms." Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal.

2009). To determine if a defendant's conduct is highly offensive, courts consider factors including "the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 606 (9th Cir.

2020). Generally, claims for invasion of privacy require an intentional act. Id.; In re Accellion Data Breach Litig., 713 F. Supp. 3d at 646–47 (holding that plaintiffs failed to establish an invasion of privacy claim where they alleged the defendant's conduct was negligent and did not otherwise allege intentional or highly offensive conduct on the defendant's part).

However, a defendant's negligent conduct may support a claim for invasion of privacy when the negligent conduct results in the disclosure of medical information. In re Ambry Genetics Data Breach Litig., 567 F. Supp. 3d at 1143. Defendants argue that Scott failed to allege that their conduct was intentional. Scott concedes that Defendants' conduct was not intentional; instead, Scott relies solely on the medical information exception to the general rule requiring intentional conduct.

Here, because no medical data was compromised, and because Scott did not allege that Defendants acted intentionally, he failed to plausibly state a claim for invasion of privacy. Scott alleges that Defendants failed to safeguard his and other Medicare Beneficiaries' PII and PHI. He does not allege any intentional conduct on behalf of Defendants. According to the notice CMS sent to Scott, the information compromised in the data breach included the individual's name, address, date of birth, phone number, social security number, Medicare beneficiary identifier, banking information, and Medicare entitlement, enrollment, and premium information.

Scott's argument that medical information was compromised in the data breach is based on his assertion that the claim identification number can be traced to specific procedures like codes used in medical billing. Importantly, however, the notice from CMS explicitly stated that no claims data was involved in the incident.

Because the information compromised in the data breach is not medical information, the Court GRANTS Defendants' Motion to Dismiss with respect to Count Four. E. California Customer Records Act This Court GRANTS Defendants' Motion to Dismiss with respect to Count Five because Scott is not a customer within the meaning of the California Customer Records Act ("CCRA").

The CCRA provides in pertinent part: A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable.

Cal. Civ. Code § 1798.82(a). The CCRA requires that the disclosure "be made in the most expedient time possible and without unreasonable delay." Id. Additionally, the CCRA requires "[a] person or business that maintains computerized data that includes personal information that the persona or business does not own" to immediately upon discovery notify the owner or licensee of the information of the breach "if the information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ.

Code § 1798.82(b). This notice requirement applies to covered entities under HIPAA. Cal. Civ. Code § 1798.82(e). Section 1798.84(b) provides a private right of action for any customer injured by a violation of the CCRA. A customer is "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business." Cal. Civ.

Code § 1798.80(c). Defendants argue that Scott and the other Medicare beneficiaries are not customers within the meaning of the CCRA; that the CCRA does not apply to Defendants because they are covered entities under HIPAA; that any delay in notifying CMS did not violate the CCRA; and that Scott was not harmed from any alleged delay in notification. Scott argues that the Medicare beneficiaries are customers within the meaning of the CCRA; that covered entities are not exempt from the requirements of § 1783.82 of the CCRA; that Defendants violated the CCRA notification requirements because they did not notify impacted individuals within the time required by HIPAA; and that Scott was harmed by Defendants' delayed notification because he would have been able to mitigate and potentially prevent the identity theft and fraud he experienced.

Here, because Scott is not Defendants' customer, he failed to state a claim under the CCRA. ASRC was contracted by CMS to process and maintain Medicare beneficiaries' personal information. ASRC later subcontracted HMS to process and maintain this data. Defendants provided a service to CMS by processing Medicare beneficiary data to determine Medicare eligibility, entitlement, and premiums.

In turn, CMS provided the Medicare beneficiaries with health care through Medicare. Medicare beneficiaries receive a service from CMS not Defendants. See In re Accellion Data Breach Litig., 713 F. Supp. 3d at 645 (holding plaintiffs were not customers of the defendant because they did not pay the defendant any money, nor did they receive a service from the defendant).

Scott's reliance on Castillo, 2016 WL 9280242, is misplaced. The court in Castillo did not apply a broad definition of the term "customer"; instead, it recognized that Cal. Civ. Code § 1798.82 simply applied to some non-customer information. Id. at *7. Indeed, that court noted that the CCRA "is primarily concerned with the protection of customer data,... and provides remedies only for customers harmed by its violation." Id. Because Scott and other Medicare beneficiaries are not customers within the meaning of the CCRA, the Court GRANTS Defendants' Motion to Dismiss Count Five.

F. California Unfair Competition Law The Court DENIES Defendants' Motion to Dismiss with respect to Count Six. California's unfair competition law ("CUCL") defines "unfair competition" as "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200 et seq. There are three different theories of liability: unlawful business practices, unfair business practices, and fraudulent business practices.

Castillo, 2016 WL 9280242 at *6 (citation omitted). Scott does not allege violation of the CUCL under the fraudulent business practice theory. 1. Unlawful Prong The Court finds that Scott adequately pled a violation of the CUCL's unfair prong.

To determine if a defendant's business practices violate the unlawful prong under the CUCL, plaintiffs often "'borrow' other laws and make claims actionable under the [CUCL]." Castillo, 2016 WL 9280242 at *6 (citing Cel-Tech Comm'ns, Inc. v. L.A. Cellular Telephone Co., 973 P.2d 527, 539–40 (Cal. 1999)).

The laws relied upon by a plaintiff under the unlawful prong need not provide the plaintiff with a right of action because the CUCL makes violations of these laws "independently actionable." Cel-Tech Comm'ns, Inc., 973 P.2d at 539–40; Castillo, 2016 WL 9280242 at *7 (holding the plaintiff adequately pled a violation of the unlawful prong where the defendant violated § 1798.82 even though plaintiff was not a customer under the CCRA's definition); Webb v. Smart Document Sols, LLC, 499 F.3d 1078, 1082–83 (9th Cir.

2007) (recognizing that a federal statute may form the basis of a CUCL unlawful prong violation without providing a private right of action). Here, Scott alleged facts sufficient to plead that Defendants' business practices violate the unlawful prong of the CUCL.

First, as stated above, Scott sufficiently pled that Defendants' conduct was negligent, that alone is sufficient to deny Defendants' motion with respect to Count Six. Scott, however, sufficiently pled

a violation to the unlawful prong through the CCRA and HIPAA.

The fact that Scott cannot bring an independent claim under either statute is not dispositive. Regarding the CCRA violation, as the court in Castillo recognized, while the CCRA gives customers a private right of action for violations under the act, it "nonetheless operates to protect some non-customer information." Castillo, 2016 WL 9280242 at *7. Scott otherwise pled facts sufficient to establish a violation to § 1798.82 of the CCRA.

Regarding the HIPAA violation, Scott alleges that Defendants failed to disclose the data breach within the sixty-day time frame under HIPAA. Either violation is sufficient to support a violation of the unlawful prong of the CUCL. Defendants argue that Scott did not allege facts sufficient to establish that they owned or licensed his computerized data or that the data was viewed by an unauthorized person.

Thus, Defendants contend Scott did not plead a violation under § 1798.82 of the CCRA. First, the Court rejects Defendants' argument that Scott did not establish that his data was viewed by an unauthorized person because Scott alleged that he experienced actual identity theft, fraud, and a decreased credit score.

The Court finds that Scott's alleged injuries alone are sufficient to establish an unauthorized person viewed and used his data. Second, the Court rejects Defendants' argument that Defendants did not own or license Scott's data.

The CCRA states that "the terms 'own' and 'license' include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates." Cal. Civ. Code § 1798.81.5(a)(2). This definition is not exclusive. People v. Experian Data Corp., No. 30-2019-01047183, 2021 Cal. Super.

LEXIS 153484, at *15 (Orange Cnty. Super. Ct. Dec. 6, 2021). Generally, the term license "means a grant of permission to do a particular thing, to exercise a certain privilege, or to carry on a particular business or to pursue a certain occupation." Id. at *15–16 (citation omitted). Defendants were granted permission to process and maintain Medicare beneficiaries' data to determine Medicare eligibility, entitlement, and premiums — i.e., permission to carry on their business.

Because the definition of license is not exclusive, and because Defendants were granted permission to carry on their business by using Medicare beneficiaries' data, the Court finds that Defendants' licensed Scott's data. 2. Unfair Prong The Court additionally concludes Scott adequately pled a violation of the CUCL's unfair prong. There are two tests to determine whether a business practice is "unfair" within the meaning of the CUCL.

First, a business practice may be "'unfair' when it 'is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." Castillo, 2016 WL 9280242 at *7 (quoting S. Bay Chevrolet v. Gen. Motors Acceptance Corp., 72 Cal. App. 4th 861, 886-87 (1999)).

To determine if this definition is met, courts "examine the practice's 'impact on its alleged victim, balanced against the reasons, justifications and motives of the alleged wrongdoer.'" Id. (citation omitted). Second, to determine if a business practice is unfair, courts "require[] that the CUCL claim to be tethered to some specific constitutional, statutory, or regulatory provisions." Id. (quoting McVicar v. Goodman Glob., Inc., 1 F. Supp. 3d 1044, 1054 (C.D.

Cal. 2014)). Federal courts apply both tests to determine if a business practice is unfair. Id. (citation omitted). Here, Scott alleged facts sufficient to establish that Defendants' business practices are unlawful under both tests.

First, as stated above, Scott has adequately pled that Defendants violated § 1798.82 of the CCRA and HIPAA's notification requirement. See Id. (holding the public policy test was satisfied where the defendant violated § 1798.82 even though plaintiff was not a customer under the CCRA's definition).

Second, balancing the impact on Scott and other Medicare beneficiaries against Defendants' justification also supports finding that Defendants' practices are unfair. The alleged impact on Scott — actual identity theft, fraud, and a decreased credit score — is not outweighed by Defendants' nonexistent justification for the alleged mishandling of data and weak security.

See Id. (finding the balancing test satisfied where the defendant "cannot offer a compelling reason or justification for its allegedly weak security protocol and mishandling of information that would outweigh the effect on plaintiffs of having false tax returns filed in their names").

Therefore, Scott adequately pled a violation of the unfair prong. 3. Injunctive Relief The Court finds that Scott has standing to bring his CUCL claim. The CUCL allows a court to enjoin "[a]ny person who engages, has engaged, or proposes to engage in unfair competition." Cal. Bus. & Prof. Code § 17203. "Any person may pursue representative claims or relief on behalf of others only if the claimant meets the standing requirements of Section 17204." Id. Section 17204 allows "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition" to pursue relief under the statute.

Cal. Bus. & Prof. Code § 17204. Defendants argue that Scott failed to allege that he suffered an injury-in-fact or that he suffered any economic damages as a result of unfair practices. Scott argues that his injuries — identity theft, fraud, and decreased credit score — are sufficient to satisfy the injury-in-fact requirement, and his time and money spent mitigating the impact of the data breach, as well as fraudulent loans, are sufficient to satisfy the damages requirement.

First, as stated above, Scott sufficiently pled an injury- in-fact, therefore the only issue regarding CUCL standing is whether he satisfies the damages requirement. Here, Scott satisfies the damage requirement. The Ninth Circuit has held that damage to a person's credit constitutes a "loss of money or property within the meaning of the CUCL." Rubio v. Capital One Bank, 613 F.3d 1195, 1204 (9th Cir.

2010). Because Scott sufficiently alleges damage to his credit, he has standing under the CUCL. The Court thus DENIES Defendants' Motion to Dismiss with respect to Count Six. G. California Confidentiality of Medical Information Act The Court GRANTS Defendants' motion to dismiss with respect to the California Confidentiality of Medical Information Act (Count Seven).

The California Confidentiality of Medical Information Act ("CCMIA") states "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization." Cal. Civ. Code § 56.10(a).

Under the statute, medical information is defined as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, reproductive or sexual health application information, mental or physical condition, or treatment." Cal. Civ.

Code § 56.05(j)(1). Defendants argue that there is no allegation whatsoever to support Scott's contention that his medical information was compromised in the data breach. Scott contends that his medical information was part of the data breach. Specifically, Plaintiff's argument is based on the theory that the Medicare Beneficiary Identification Number or claim identification number could be traced to specific procedures, like codes used in medical billing.

Here, because no claims data was compromised in the data breach, Scott failed to allege facts sufficient to plausibly establish a violation under the CCMIA. Following the data breach, the CMS sent a notice to Scott and other effected individuals that included the information that was potentially compromised. This information included the individual's name, address, date of birth, phone number, social security number, Medicare beneficiary identifier, banking information, and Medicare entitlement, enrollment, and premium information.

This information, while individually identifiable, does not fall within the meaning of medical information under the CCMIA because it does not reference Scott's medical history, mental or physical condition, treatment, or medical care applications. At oral argument counsel for Scott argued that Medicare claims data fits within the CCMIA definition for medical information.

Importantly, however, the notice from CMS explicitly stated that no claims data was involved in the incident. Because the information compromised in the data breach does not constitute medical

information under the CCMIA, the Court GRANT Defendants' motion to dismiss with respect to Count Seven. H. Declaratory Judgment The Court DENIES Defendants' Motion to Dismiss with respect to Count Eight.

Pursuant to the Declaratory Judgment Act, a federal district court "may declare the rights and other legal relations of any interested party seeking such declaration whether or not further relief is or could be sought." 28 U.S.C. § 2201(a).

The two principal criteria guiding the policy in favor of rendering declaratory judgments are (1) when the judgment will serve a useful purpose in clarifying and settling the legal relations in issue, and (2) when it will terminate and afford relief from the uncertainty, insecurity, and controversy giving rise to the proceeding. Edelbrock LLC v. Genesis Grp.

Int'l (USA), Inc., 119 F. Supp. 3d 1168, 1173 (C.D. Cal. 2015). Often, "the cause of action accompanying a request for declaratory judgment is breach of contract, for which the declaratory judgment serves as a remedy....

In such cases, the declaratory judgment may be used to affirm the existence of a breach of contract or to clarify any attending contractual obligations." Siino v. Foresters Life Ins. & Annuity Co., 133 F.4th 936, 945 (9th Cir. 2025).

However, a declaratory judgment claim may be "unnecessary where an adequate remedy exists under some other cause of action." In re Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1138 (N.D. Cal. 2018); Reyes v. Nationstar Mortg. LLC, 2015 WL 4554377, at *7 (N.D. Cal. July 28, 2015). But, "[t]he existence of another adequate remedy does not preclude a declaratory judgment that is otherwise appropriate." Fed.

R. Civ. P. 57; In re Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d at 1138. For example, courts have allowed declaratory judgment claims to proceed when they seek forward looking declarations regarding the enforceability of a contract's terms. See In re Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d at 1139; Pitkin v. State Farm Gen.

Ins. Co., 2023 WL 11990316, at *9–10 (N.D. Cal. July 25, 2023)(allowing claim to proceed because the plaintiffs' claims remained open, plaintiffs were still insured by defendant, and the declaration "would govern ongoing interactions between plaintiffs and defendants" and clarify their legal rights); Hameed-Bolden v. Forever 21 Retail, Inc., 2018 WL 6802818, at *9 (C.D.

Cal. Oct. 1, 2018)(denying motion to dismiss declaratory judgment claim when plaintiffs alleged their information remained vulnerable and the steps defendants needed to take to remedy the data breach). Thus, a declaratory judgment claim is not duplicative if a plaintiff seeks prospective relief, such as a prospective declaration of a plaintiff's rights and duties under a contract.

Alta Devices, Inc. v. LG Elecs., Inc., 343 F. Supp. 3d 868, 890 (N.D. Cal. 2018). Here, Defendants argue that Scott's claim for declaratory relief fails because it is duplicative of his claims for negligence and breach of fiduciary duty, and thus serves no useful purpose. ECF No. 67.

In contrast, Plaintiff Scott contends that courts routinely allow plaintiffs to pursue alternative remedies even if the relief overlaps with other claims that might survive a motion to dismiss. ECF No. 73. Additionally, Plaintiff argues that in data breach cases, where it is too early to tell if the defendant will fix the alleged security issues, declaratory relief may be necessary to prevent future harm.

Id. At the pleading stage, the Court finds Scott's declaratory judgment claim may proceed. Plaintiff sufficiently alleges that he cannot opt out of providing his PHI because it is a condition for receiving Medicare services. Further, he contends that Defendants have not made adequate corrective action to prevent future data breaches.

Thus, the declaration would govern ongoing interactions between Plaintiff and defendants and clarify their legal rights. The Court DENIES Defendants' motion to dismiss with respect to Count Eight. Vv. CONCLUSION For the foregoing reasons, the Court GRANTS IN PART and DENIES IN PART Defendants' Motion to Dismiss [ECF No. 66]. Specifically, the Court DENIES Defendants' Rule 12 (b) (1) Motion; GRANTS Defendants' Motion to Dismiss Count Two (breach of implied contract), Count Three (breach of fiduciary duty), Count Four (invasion of privacy), Count Five (CCRA), Count Seven (CCMIA); and DENIES Defendants' Motion to Dismiss with respect to the standing issue, Count One (negligence), Count Six (CUCL), and Count Eight (declaratory judgment).

Further, Defendants' Motions for Protective Orders [ECF Nos. 78, 79] seeking to stay discovering pending a ruling on the subject motion are DENIED AS MOOT. It is so ORDERED. The Clerk is directed to transmit copies of this Memorandum Opinion and Order to counsel of record by the CM/ECF system. DATED: March 31, 2026 Tom 8 Bla THOMAS S. KLEEH, CHIEF JUDGE NORTHERN DISTRICT OF WEST VIRGINIA 41