NOT FOR PUBLICATION

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

IN RE: BANNER HEALTH DATA BREACH LITIGATION	No. CV-16-02696-PHX-SRB **ORDER**

At issue is Defendant Banner Health's Motion to Dismiss ("MTD") (Doc. 76).

I. BACKGROUND

This case arises out of a data breach incident in June 2016, during which hackers accessed several of Defendant's networks and servers containing electronically stored personally identifying information ("PII"), such as names, addresses, birthdates, and social security numbers; protected health information ("PHI"), such as medical histories; and payment card information ("PCI") belonging to nearly four million patients, insurance plan members, plan beneficiaries, payment card users, and healthcare providers. (Doc. 74, Plaintiffs' Consolidated Am. Class Action Compl. ("Am. Compl.") ¶¶ 2, 6-8.) The data breach began on June 17, 2016, when the hackers first gained access to Defendant's network. (*Id.* ¶ 191.) Defendant discovered the breach on June 29, 2016, while investigating unusual slowness on various servers, and subsequently engaged a company to provide response services and investigate the breach. (*Id.* ¶¶ 223-24.) The investigation revealed that a "financially motivated threat group" committed the breach. (*Id.* ¶¶ 187-88.) The group's previous criminal activities have generally involved the theft

of identity information that can be used to make money. (*Id.*) On August 3, 2016, Defendant publicly announced the breach and stated that breach notification letters would be sent to all affected individuals by September 9, 2016. (*Id.* ¶ 232.)

Defendant is a Phoenix-based healthcare network consisting of hospitals, clinics, surgery centers, an insurance company and other entities, and it operated health entities in Alaska, Arizona, California, Colorado, Nebraska, Nevada, and Wyoming during the relevant time period. (*Id.* ¶¶ 60-61.) Plaintiffs Howard Chen, Betty Clayton, Stacey Halpin, Kim Maryniak, Summer Sadira, and Stan Griep[1] (collectively "Plaintiffs") brought this putative class action on behalf of themselves and all patients ("Patient Plaintiffs"), insurance plan members ("Insurance Plan Plaintiffs"), healthcare providers, and employees ("Employee Plaintiffs") whose PII and/or PHI was maintained on Defendant's network and who were mailed a breach notification letter as well as all individuals whose PCI was transmitted on Defendant's compromised server ("Payment Card Plaintiffs") and who were mailed a breach notification letter. (*Id.* ¶¶ 267.)[2] Plaintiffs allege that the hackers were able to access their PII, PHI, and PCI because of Defendant's failure to take adequate precautions such as multi-factor authentication, firewalls, adequate encryption, and so forth to protect it. (*Id.* ¶¶ 5-6.) Plaintiffs Halpin and Maryniak allege that their confidential information has already been misused for things such as opening fraudulent bank accounts, filing a false tax return, and fraudulently using credit cards, and that they have spent time and money to correct the misuse and will continue to spend time and money to prevent further misuse. (*Id.* ¶¶ 33-36, 43-44). Plaintiffs Chen, Clayton, Sadira, and Griep allege that although they have not yet detected any misuse of their PII, PHI, or PCI, they have spent and will continue to spend time and money to safeguard against their increased risk of identity theft. (*Id.* ¶¶ 17, 23-

---

[1] Plaintiffs Chen, Clayton, Halpin, and Maryniak are citizens and residents of Arizona. (Am. Compl. ¶¶ 9, 18, 26, 37.) Plaintiffs Sadira and Griep are citizens and residents of Colorado. (*Id.* ¶¶ 45, 51.)

[2] All named Plaintiffs were either patients, employees, or insurance plan members, although some also used payment cards at Defendant's facilities.

25, 49-50, 55.) Plaintiffs further allege that Defendant was aware that its "data systems are high value targets for cyber criminals and at high risk for a data breach" but that, since 2012, Defendant's "information security measures have been objectively unreasonable and deficient" in light of industry standards and legal requirements. (*Id.* ¶¶ 136, 150.) Plaintiffs also allege that they were all parties to medical care, employment, or insurance contracts with Defendant in which Defendant promised to secure Plaintiffs' PII and PHI. (*Id.* ¶¶ 91-110.) Plaintiffs have brought seven causes of action against Defendant: negligence, negligence per se, breach of contract, breach of the implied covenant of good faith and fair dealing, breach of implied duty to perform with reasonable care, unjust enrichment, and violation of the Arizona Consumer Fraud Act ("ACFA"). (¶¶ 276-346.) Defendant now moves to dismiss for lack of standing and for failure to state a claim. (MTD at 1.)

II. LEGAL STANDARDS AND ANALYSES

A. Standing

Defendant argues that four of the Plaintiffs have failed to adequately allege standing because they have not yet suffered identity theft. (MTD at 3-4.) In considering a Rule 12(b)(1) motion to dismiss for lack of jurisdiction, the Court takes the allegations in Plaintiffs' Amended Complaint as true. *Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004) (citations omitted). It is Plaintiffs' burden to show "that the facts alleged, if proved, would confer standing upon [them]." *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1140 (9th Cir. 2003). Under Article III of the Constitution, a plaintiff does not have standing unless he can show (1) an "injury in fact" that is concrete and particularized and actual or imminent (not conjectural or hypothetical); (2) that the injury is fairly traceable to the challenged action of the defendant; and (3) that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). When dealing with behavior that is alleged to increase the risk of future injury, as here, the future injury must be "certainly impending" and not merely conjectural. *Clapper v. Amnesty Int'l*, 568 U.S. 398, 409 (2013).

The Ninth Circuit has previously concluded that a plaintiff meets the injury-in-fact requirement by alleging an increased risk of identity theft due to the theft of his or her PII even without alleging that any actual identity theft has occurred. *Krottner v. Starbucks Corp.*, 328 F.3d 1139, 1140 (9th Cir. 2010). In *Krottner*, several Starbucks employees sued based on their increased risk of identity theft when a laptop was stolen containing their PII, such as names, addresses, and social security numbers. *Id.* The court concluded that because the laptop had actually been stolen, the plaintiffs' increased risk of identity theft was no longer conjectural, but real and immediate. *Id.* at 1143. Defendant argues that although *Krottner* has not been overruled, the Supreme Court's holding in *Clapper* requires a finding that Plaintiffs have failed to allege standing in this case. (MTD at 5; Doc. 95, Def.'s Reply in Supp. of MTD ("Reply") at 1-3.) In *Clapper*, the Supreme Court reversed the Second Circuit's finding that United States' citizens engaged in international communications had standing to challenge the Foreign Intelligence Surveillance Act. 568 U.S. at 401-02. The Court noted that a person must show that a future injury is "certainly impending" to satisfy standing requirements, rather than the "objectively reasonable likelihood" standard required by the Second Circuit. *Id.* at 409. The Supreme Court, however, made clear that by requiring an injury to be "certainly impending", it was not creating any new standing requirements; rather, it reaffirmed and clarified those already in place. *See id.* ("[W]e have repeatedly reiterated that threatened injury must be *certainly impending* to constitute injury in fact." (quotation omitted) (emphasis in original)).

"[W]here the reasoning or theory of our prior circuit authority is clearly irreconcilable with the reasoning or theory of intervening higher authority, a [district court] should consider itself bound by the latter and controlling authority, and should reject the prior circuit opinion as having been effectively overruled." *United States v. Slade*, 873 F.3d 712, 715 (9th Cir. 2017) (quoting *Miller v. Gammie*, 335 F.3d 889, 893 (9th Cir. 2003) (en banc)). The Court concludes, however, that the reasoning in *Krottner* is not clearly irreconcilable with the reasoning in *Clapper*. Although the court in *Krottner* concluded that the harm presented by the stolen laptop was "real and immediate" as

opposed to "certainly impending", the Court cannot conclude that there is a functional difference between the two characterizations. *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014). *Clapper* is further distinguishable from *Krottner* and the allegations at hand because *Clapper* applied an "especially rigorous" standing analysis due to separation-of-powers concerns because the plaintiffs in that case claimed that an act of government was unconstitutional. 568 U.S. at 408-09. There is no such concern that would justify special rigor here. Furthermore, the Supreme Court noted that the plaintiffs in *Clapper* were unable to show not only what the government's surveillance targeting practices were, but also that they would be subject to surveillance under the statute challenged rather than another statute. *Id.* at 412-13. Plaintiffs, on the other hand, have alleged that their information was targeted and acquired by a financially-motivated hacking group known for misusing personal information for financial gain. This exceeds what was required in *Krottner* since the plaintiffs there did not make any allegations regarding who stole their information or what their motives might have been. Plaintiffs' allegations in this regard create at least a plausible inference that the harms they fear are "certainly impending." *See Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693-94 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information?"); *Galaria v. Nationwide Mutual Ins. Co.*, 663 Fed. App'x 384, 388 (6th Cir. 2016) ("There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals."); *In re Adobe*, 66 F. Supp. 3d at 1216 ("[A]fter all, why would hackers target and steal personal customer data if not to misuse it?"). Therefore, the Court concludes that all of the Plaintiffs have adequately alleged a certainly impending injury and denies Defendant's Motion on this ground.

B. Failure to State a Claim

Defendant also argues that Plaintiffs' Complaint should be dismissed for failure to state a claim. (MTD at 1.) Rule 12(b)(6) dismissal for failure to state a claim can be based on either (1) the lack of a cognizable legal theory or (2) insufficient facts to support a

cognizable legal claim. *Conservation Force v. Salazar*, 646 F.3d 1240, 1242 (9th Cir. 2011), *cert. denied*, *Blasquez v. Salazar*, 132 S. Ct. 1762 (2012). In determining whether an asserted claim can be sustained, "[a]ll of the facts alleged in the complaint are presumed true, and the pleadings are construed in the light most favorable to the nonmoving party." *Bates v. Mortg. Elec. Registration Sys., Inc.*, 694 F.3d 1076, 1080 (9th Cir. 2012). "[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.'" *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007) (quoting *Scheuer v. Rhodes*, 416 U.S. 232, 236 (1974)). However, "for a complaint to survive a motion to dismiss, the nonconclusory 'factual content,' and reasonable inferences from that content, must be plausibly suggestive of a claim entitling the plaintiff to relief." *Moss v. U.S. Secret Serv.*, 572 F.3d 962, 969 (9th Cir. 2009) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). In other words, the complaint must contain enough factual content "to raise a reasonable expectation that discovery will reveal evidence" of the claim. *Twombly*, 550 U.S. at 556.

i. Contract Claims

a. Breach of Contract

Defendant concedes that it did have various contractual relationships with Plaintiffs but argues that Plaintiffs have failed to state a claim for breach of contract because the agreements between the parties were for the provision of healthcare and insurance and none of the documents or policies cited by Plaintiffs contained express promises regarding the quality of Defendant's data security measures or promises to keep Plaintiffs' PII and PHI secure. (MTD at 5-11.) Defendant also argues that even if such promises do exist, they are not supported by consideration because Defendant was already obligated by law to keep their information secure. (MTD at 7.) "For a valid contract to exist, there must have been an offer, acceptance of the offer, consideration, sufficient specification of terms so that the obligations involved can be ascertained, and the parties must have intended to be bound by the agreement." *Day v. LSI Corp.*, 174 F.

Supp. 3d 1130, 1153 (D. Ariz. 2016) (citations omitted). Under Arizona law, "the performance or promise to do something that a party is already legally obligated to do is not valid consideration for a contract." *Snow v. W. Sav. & Loan Ass'n*, 730 P.2d 197, 202 (Ariz. Ct. App. 1985), *vacated in part on other grounds*, 730 P.2d 204 (Ariz. 1986) (citing *J. D. Halstead Lumber Co. v. Hartford Acc. & Indem. Co.*, 298 P. 925, 927 (Ariz. 1931)). Contractual terms are reasonably certain, or ascertainable, if the agreement "provides 'a basis for determining the existence of a breach and for giving an appropriate remedy.'" *Schade v. Diethrich*, 760 P.2d 1050, 1059 (Ariz. 1988) (quoting Restatement (Second) of Contracts § 33(2)).

Plaintiffs argue that there are three written contracts with incorporated privacy policies in which Defendant promised to safeguard their personal information: (1) the Summary Plan Description between Defendant and its healthcare plan members along with Defendant's "Privacy Practices in Banner Plans"; (2) the Medical Treatment Agreement between Defendant and its patients along with Defendant's "Notice of Privacy Practices"; and (3) Defendant's Employee Handbook along with its "Workforce Confidentiality Policy." (Doc. 83, Pls.' Resp. in Opp'n to MTD ("Resp.") at 7-8.) The Court first examines the agreements between Defendant and the Patient and Insurance Plan Plaintiffs. The Court need not address whether Plaintiffs have sufficiently alleged the proper incorporation of the privacy policies at issue into their respective written agreements because, even if they are properly incorporated, they do not contain reasonably ascertainable express promises to maintain data security above and beyond Defendant's preexisting duties under the law.

For example, Defendant's "Notice of Privacy Practices", which Plaintiffs allege is part of Defendant's contract with all of its patients and insurance plan members, states:

> Banner is committed to protecting the confidentiality of information about you, and is required by law to do so. This notice describes how we may use information about you within Banner Health and how we may disclose it to others outside Banner. We will notify you if there is a breach of your *unsecured* protected health information.

(Doc. 76-2, Ex. 2 – Notice of Privacy Practices for Banner Health at 1 (emphasis

added).)[3] Although this language could arguably be read as a promise to keep patient information confidential, it cannot be read as a promise to do anything above and beyond what is already required by law. Defendant states that it is committed to protecting the information *and* is required by law to do so. Nothing here suggests a reasonably ascertainable promise to do anything not already required by law. As such, this promise is simply not supported by consideration because Defendant was already under a preexisting legal duty to protect Plaintiff's information. *Hisel v. Upchurch*, 797 F. Supp. 1509, 1521 (D. Ariz. 1992) ("[A] promise to perform a pre-existing duty is insufficient consideration."); 45 C.F.R. §§ 160.101-160.552, 164.102-164.534 (regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requiring entities such as Defendant to protect PHI and secure electronically stored PHI). Furthermore, when referencing the possibility of a data breach, Defendant acknowledges the possibility that some data may be unsecured and promises only to notify those affected. Plaintiffs have not alleged that Defendant failed to do so.

Plaintiffs allege that the Summary Plan Description and its accompanying "Privacy Practices in Banner Plans" contain nearly identical language to the Notice of Privacy Practices. (Am. Compl. ¶¶ 102-03.) The Court finds that the alleged promises in the Summary Plan Description suffer from the same defects as those in the Notice of Privacy Practices in that they make no reasonably ascertainable promise above and beyond that which Defendant was already required to do by law. Therefore, Plaintiffs have failed to allege that the contracts between Defendant and the Patient Plaintiffs and Insurance Plan Plaintiffs contain an enforceable express contract to keep their information secure.

The Employee Plaintiffs also claim that Defendant promised to keep their PII confidential in their employment agreements. (Am. Compl. ¶¶ 105-110; Resp. at 8.) All

---

[3] Defendant attached a full copy of its Notice of Privacy Practices to its Motion. The Court has discretion to consider documents referenced in the Complaint when ruling on a motion to dismiss and finds it appropriate to do so here. *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1159-60 (9th Cir. 2012).

of the language alleged by Plaintiffs, however, expresses Defendant's employees' obligations to keep information learned at work confidential, rather than any obligations for Defendant to keep information confidential. Plaintiffs allege that Defendant's Employee Handbook reads:

> Patient care information is considered confidential by law and we have an obligation to protect our patients' rights to confidentiality. . . . Any materials developed by employees during work hours will remain the property of Banner and are to be considered confidential information. . . . Our obligation to protect confidential information is so important that every employee is expected to honor privacy and confidentiality.
>
> . . . Banner adheres to HIPAA as it applies to our activities as a health care provider and health plan, and employees are expected to comply with HIPAA as well. . . . Violations of HIPAA are very serious and may result in corrective action, up to and including termination.

(Am. Compl. ¶¶ 106-07). Plaintiffs also allege that the Banner Workforce Confidentiality Policy is incorporated by reference into the Employee Handbook. (*Id.* ¶¶ 108-09.) That Policy states:

> Banner has a legal and ethical responsibility to safeguard confidential information. Banner will comply with all laws and regulations relating to confidentiality and will protect oral, paper, and electronic confidential information. . . . Banner's obligation to protect confidential information is so important that every member of Banner must agree to honor privacy and confidentiality during and beyond employment.

(*Id.* ¶ 108.) Assuming that the Employee Handbook and Banner Workforce Confidentiality Policy are contracts, none of the obligations outlined in the alleged language are owed by Defendant to its employees; rather, every alleged duty is owed by Defendant's employees to Defendant as a condition of employment. Therefore, these allegations are insufficient to support a claim that Defendant breached an express agreement with the Employee Plaintiffs by failing to secure their information. Accordingly, the Court grants Defendant's Motion to dismiss Plaintiffs' breach of contract claim.

b. Implied Covenant of Good Faith and Fair Dealing

Plaintiffs argue that even if Defendant made no express promises to maintain adequate data security, Defendant was still obligated to keep their information secure

under the implied covenant of good faith and fair dealing because they were required to give Defendant their PII and PHI in order to obtain employment, healthcare, and insurance. (Resp. at 13.) Arizona law implies a covenant of good faith and fair dealing in every contract. *Wells Fargo Bank v. Ariz. Laborers, Teamsters & Cement Masons Local No. 395 Pension Trust Fund*, 38 P.3d 12, 28 (Ariz. 2002) (en banc). "The implied covenant of good faith and fair dealing prohibits a party from doing anything to prevent other parties to the contract from receiving the benefits and entitlements of the agreement" and "extends beyond the written words of the contract." *Id.* at 28-29. A party can breach this covenant "if he or she acts in a manner that denies the other party the reasonably expected benefits of the contract" or "uses discretion for a reason outside the contemplated range—a reason beyond the risks assumed by the party claiming a breach." *Coulter v. Grant Thornton, LLP*, 388 P.3d 834, 842 (Ariz. Ct. App. 2017) (internal quotations and citations omitted). Plaintiffs argue that adequate protection of their PII and PHI was a reasonably expected benefit of their contracts with Defendant. (Resp. at 13.) But the implied covenant of good faith and fair dealing ensures that parties do not frustrate already-existing contract terms; it does not create new ones. *11333 Inc. v. Certain Underwrtiers at Lloyd's*, London, 261 F. Supp. 3d 1032, 2017 WL 2556755, at *14 (D. Ariz. June 13, 2017) ("The implied covenant of good faith and fair dealing is not a vehicle for creating contractual terms that the parties did not otherwise agree to; it protects the existing terms from subversion."). Because the Court concluded above that Plaintiffs have not adequately alleged an enforceable promise to keep information secure, Defendant cannot have breached the implied covenant of good faith and fair dealing by failing to do so. Therefore, the Court grants Defendant's Motion to dismiss this claim.

c. Implied Duty to Perform with Reasonable Care

Defendant argues that it cannot have breached the implied duty to perform with reasonable care because the implied duty only applies to the performance of express obligations within a contract. (MTD at 11-12.) Plaintiffs argue that they have sufficiently alleged that Defendant expressly agreed to secure their data. As explained above, the

Court disagrees. The implied duty of reasonable care, where it is recognized[4], applies only to express services provided for in a contract. *Mid-Century Ins. Co. v. InsulVail, LLC*, 592 F. App'x 677, 681-84 (10th Cir. 2014) (applying Colorado law). Because the Court concluded above that Plaintiffs have failed to allege adequately an express contractual agreement to provide data security, their claim for breach of the implied duty to perform with reasonable care also fails. Therefore, the Court grants Defendant's Motion to dismiss this claim.

d. Unjust Enrichment

Defendant argues that Plaintiffs cannot maintain a claim for unjust enrichment because they have already alleged the existence of contracts between the parties for the provision of medical services and insurance. (MTD at 12.) "To recover on a theory of unjust enrichment, [Plaintiffs] must allege and prove that [Defendant] acquired the money under circumstances which renders [Defendant's] retention of the money inequitable." *Johnson v. Am. Nat. Ins. Co.*, 613 P.2d 1275, 1279 (Ariz. Ct. App. 1980).

> To establish a claim for unjust enrichment, a party must show: (1) an enrichment; (2) an impoverishment; (3) a connection between the enrichment and the impoverishment; (4) the absence of justification for the enrichment and the impoverishment; and (5) the absence of a legal remedy.

Trustmark Ins. Co. v. Bank One, Arizona, NA, 48 P.3d 485, 491 (Ariz. Ct. App. 2002). Plaintiffs allege that they paid money to Defendant for insurance plan premiums and healthcare service, that part of the money was supposed to be used for the administrative costs of data security, and that Defendant failed to provide adequate data security. (Am. Compl. ¶ 333.) These allegations are sufficient to support a claim for unjust enrichment. *See In re Premera Blue Cross Customer Data Security Breach Litigation*, 198 F. Supp. 3d 1183, 1200-01 (D. Or. 2016) ("Plaintiffs allege that they made payments to Premera and that under the circumstances it is unjust for Premera to retain the benefits received without payment. This is sufficient to withstand a motion to dismiss."). Although

[4] The parties have not cited, nor has the Court located, any case stating that the duty of reasonable care is recognized under Arizona law.

Defendant is correct that an express contract regarding data security would preclude a claim for unjust enrichment, Plaintiffs are not precluded from pleading alternative theories of recovery. "The mere existence of a contract governing the dispute does not automatically invalidate an unjust enrichment alternative theory or recovery." *Adelman v. Christy*, 90 F. Supp. 2d 1034, 1045 (D. Ariz. 2000). "A theory of unjust enrichment is unavailable only to a plaintiff if that plaintiff has already *received* the benefit of her contractual bargain." *Id.* (emphasis in original). Plaintiffs here allege they have not. Therefore, the Court denies Defendant's Motion to dismiss this claim.

ii. ACFA Claim

Plaintiffs allege that Defendant violated the ACFA by failing to disclose "that its computer systems and data security practices were inadequate to safeguard [their] PII, PHI, and PCI, and that the risk of a data breach or theft was highly likely." (Am. Compl. ¶ 344.) Defendant argues that Plaintiffs have failed to allege adequately a claim under the ACFA because their allegations are not sufficiently particular. (MTD at 13.) The ACFA prohibits fraudulent, deceptive, or misleading conduct in connection with the sale of consumer goods and services. A.R.S. § 44-1522(A). "To prevail [on an ACFA claim], a plaintiff must establish that (1) the defendant made a misrepresentation in violation of the Act, and (2) defendant's conduct proximately caused plaintiff to suffer damages." *Cheatham v. ADT Corp.*, 161 F. Supp. 3d 815, 825 (D. Ariz. 2016) (citing *Parks v. Macro-Dynamics, Inc.*, 591 P.2d 1005, 1008 (Ariz. Ct. App. 1979)). Parties can be liable for affirmative misrepresentations and omissions. *Maurer v. Cervenik-Anderson Travel, Inc.*, 890 P.2d 69, 72 (Ariz. Ct. App. 1994). Claims arising under the ACFA pertain to fraud and are thus subject to the pleading requirements of Rule 9(b) of the Federal Rules of Civil Procedure. "[A] party must state with particularity the circumstances constituting fraud." Fed. R. Civ. P. 9(b); *see also Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) ("It is established law, in this circuit and elsewhere, that Rule 9(b)'s particularity requirement applies to state-law causes of action."). "Averments of fraud must be accompanied by 'the who, what, when, where, and how' of the misconduct

charged," and a "plaintiff must set forth what is false or misleading about a statement, and why it is false." *Vess*, 317 F.3d at 1106 (citations omitted). The allegations must be "specific enough to give defendants notice of the particular misconduct so that they can defend against the charge and not just deny that they have done anything wrong." *Id.*

Defendant argues that Plaintiffs' claim fails because they did not identify with specificity the documents alleged to be the source of the misrepresentations. (MTD at 13.) Plaintiffs argue that because they are alleging only fraud by omission, the pleading standards are relaxed. (Resp. at 16.) They further argue that they identified several notices in which information regarding Defendant's allegedly inadequate data security could have been provided, such as the Notice of Privacy Practices, the Medical Treatment Agreement, and the Summary Plan Description. (*Id.*; Am. Compl. ¶¶ 95, 99, 103.) "[A] plaintiff in a fraud-by-omission suit faces a slightly more relaxed burden, due to the fraud-by-omission plaintiff's inherent inability to specify the time, place, and specific content of an omission in quite as precise a manner." *Schellenbach v. GoDaddy.com LLC*, No. CV-16-00746-PHX-DGC, 2017 WL 192920, at *2 (D. Ariz. Jan. 18, 2017) (quoting *Tait v. BSH Home Appliances Corp.*, No. SACV 10-00711 DOC, 2011 WL 3941387, at *2 (C.D. Cal. Aug. 31, 2011)). The Court finds that Plaintiffs have met this burden in this case. They identified documents pertaining to Defendant's privacy practices that did not contain information about Defendant's allegedly inadequate security practices. *See id.* at *4 (concluding that identifying advertisements lacking the allegedly material information was sufficiently particular to plead fraud by omission under the ACFA). Therefore, the Court concludes that Plaintiffs have identified the alleged omissions with sufficient particularity.

Defendant also argues that Plaintiffs failed to allege that any of them actually read or relied on any statements about data security when deciding to purchase healthcare or insurance and that they therefore could not have been misled by any alleged omissions. (MTD at 13.) Defendant is correct that Plaintiffs did not plead that any of them actually read any of the notices mentioned in the Complaint when deciding whether to purchase

services from Defendant. (*See* Am. Compl. ¶¶ 337-46.) As such, there is a question of causation—if Defendant had disclosed its data security weaknesses, would Plaintiffs have been aware of these disclosures? Plaintiffs allege that they "were ignorant of the truth and relied on the concealed facts and incurred damages as a consequent and proximate result." (Am. Compl. ¶ 345.) Accepting this as true, as the Court must at this stage of the proceedings, the Court concludes that this allegation raises a plausible inference that Plaintiffs were aware of Defendant's privacy policies and would have acted differently if they had been aware of the alleged security deficiencies. *See In re Premera*, 198 F. Supp. 3d at 1194 ("Plaintiffs allege that had Premera disclosed its 'true' data security practices, the Policyholder Plaintiffs never would have purchased their health insurance from Premera in the first place. This is a sufficient allegation of materiality and reliance."). Therefore, the Court will not dismiss Plaintiffs' ACFA claim on this ground.

Finally, Defendant argues that Plaintiffs failed to allege that Defendant intentionally misled them through its omission. (MTD at 13-14.) Plaintiffs argue that under the ACFA, a plaintiff need only show intent to do the act involved rather than specific intent to deceive. (Resp. at 18.) The Court agrees with Plaintiffs. "It is well-settled that a person or entity need not intend to deceive to violate the [ACFA]." *Powers v. Guar. RV, Inc.*, 278 P.3d 333, 338 (Ariz. Ct. App. 2012) (citing *State ex rel. Babbitt v. Goodyear Tire & Rubber Co.*, 626 P.2d 1115, 1118 (Ariz. Ct. App. 1981)). The cases cited by Defendant for the opposite conclusion are inapposite. The court in *Tavilla v. Cephalon, Inc.* was discussing the requirements for showing common-law fraud when it stated that specific intent to deceive was required, and the court in *In re Toyota Motor Corp.* was not dealing with any claims under the ACFA. *Tavilla v. Cephalon, Inc.*, 870 F. Supp. 2d 759, 774 (D. Ariz. 2012); *In re Toyota Motor Corp.*, 754 F. Supp. 2d 1145 (C.D. Cal. 2010). Plaintiffs alleged that Defendant was aware that its data security was insufficient and yet did not disclose this fact to potential customers. This raises a plausible inference that Defendant intended to omit that information from its data privacy policies. Therefore, the Court denies Defendant's Motion to dismiss Plaintiffs' ACFA

claim.

iii. Negligence Claims

Defendant argues that Plaintiffs have failed to show causation and damages sufficient to sustain their negligence claims. (MTD at 14.) It argues that Plaintiffs may not recover damages for money spent to prevent future identity theft and that, in any case, all alleged harm is purely economic and therefore ineligible for recovery under tort law. (MTD at 14-16.) "To establish a claim for negligence, a plaintiff must prove four elements: (1) a duty requiring the defendant to conform to a certain standard of care; (2) a breach by the defendant of that standard; (3) a causal connection between the defendant's conduct and the resulting injury; and (4) actual damages." *Gipson v. Kasey*, 150 P.3d 228, 230 (Ariz. 2007) (en banc). Whether a duty exists is a matter of law while "[t]he other elements, including breach and causation, are factual issues usually decided by the jury." *Id.*

Defendant argues that Plaintiffs cannot show that they have been damaged because they do not allege that they have suffered any costs which were not reimbursed. (MTD at 14.) Plaintiffs argue that identity theft, out-of-pocket expenses to mitigate the risk of future identity theft, Plaintiffs' increased risk of harm in itself, and the loss of value of their PII all constitute actual injuries for which they may recover damages. (Resp. at 19-22.) The Court agrees with Plaintiffs that they have properly alleged at least some damages. First, the Plaintiffs who allege they have suffered actual misuse of their personal information have clearly suffered an actual injury for which they may recover. *Stollenwerk v. Tri-West Health Care Alliance*, 254 Fed. App'x 664, 667-68 (9th Cir. 2007) (individual who experienced identity theft after a burglary stated a claim for negligence). Regarding out-of-pocket expenses to mitigate the future risk of identity theft, Arizona courts follow the Restatement absent contradictory controlling authority, which provides:

> A person whose legally protected interests have been endangered by the tortious conduct of another is entitled to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened.

Restatement (Second) of Torts § 919(1) (1979); *Dixon v. City of Phoenix*, 845 P.2d 1107, 1116 (Ariz. Ct. App. 1992). Plaintiffs have alleged that Defendant's failure to adequately secure their PII, PHI, and PCI has put them in danger of identity theft and that they have spent and will continue to spend time and money to guard against this risk. (Am. Compl. ¶¶ 17, 25, 36, 44, 50, 55, 284-85.) Therefore, these expenses are also adequately alleged damages from Defendant's actions.[5]

Plaintiffs' damages are also not precluded by the economic loss rule. When applicable, "[t]he economic loss rule bars a party from recovering economic damages in tort unless accompanied by physical harm, either in the form of personal injury or secondary property damage." *Carstens v. City of Phoenix*, 75 P.3d 1081, 1084 (Ariz. Ct. App. 2003). The economic loss rule arose as a way of distinguishing claims that arise in tort or in contract, and the principal public policy underlying the rule recognizes "that contract law and tort law each protect distinct interests." *Id.* at 1084. Contract law focuses on "standards of quality as defined by the parties in their contract" while tort law "seeks to protect the public from harm to person or property." *Id.* Generally, tort law provides "duty-based recovery" while contract law allows for "promise-based recovery." *Id.* The economic loss rule, however, "cannot simply be applied as a blanket restriction precluding tort-based lawsuits by plaintiffs who have suffered solely economic loss." *Evans v. Singer*, 518 F. Supp. 2d 1134, 1139 (D. Ariz. 2007). Indeed, "[t]ort law has traditionally protected individuals from a host of wrongs that cause only monetary damage." *Giles v. Gen. Motors Acceptance Corp.*, 494 F.3d 865, 875 (9th Cir. 2007). In Arizona, the economic loss rule has typically only been applied in the areas of construction defects and products liability. *Evans*, F. Supp. 2d at 1142. This case does not concern those areas of law. Furthermore, Plaintiffs have as of yet failed to allege adequately the existence of a contract governing data security between the parties,

---

[5] The Court does not address whether the increased risk of identity theft or the loss in value of Plaintiffs' PII are damages for which they may seek recovery because the Court has concluded that the other damages alleged by Plaintiffs are sufficient to withstand a motion to dismiss.

making it inappropriate to dismiss their claim for negligence at this stage in the litigation based on a rule designed solely for the purpose of distinguishing contractual and tort duties. Therefore, the Court will not dismiss Plaintiffs' negligence claims for this reason.

Finally, Defendant argues that Plaintiffs have not pled sufficient facts to show causation. (MTD at 16.) The Court disagrees. Plaintiffs plead that Defendant maintained inadequate security practices which left their PII, PHI, and PCI exposed; that financially motivated criminals who target this kind of data stole their PII, PHI, and PCI; and that the theft has led to identity theft and an increased risk of identity theft requiring them to take protective actions. Although this does not conclusively prove that Defendant's actions caused Plaintiffs' harm, proof is not required at this stage in the proceedings. There is at least a plausible inference that the identity theft alleged by two of the Plaintiffs would not have happened but-for Defendant's inadequate data security. Furthermore, there is a plausible inference that the rest of Plaintiffs are now at an increased risk of identity theft which they are incurring costs to prevent. *See In re Anthem, Inc. Data Breach Litigation*, 2016 WL 3029783, at *16 (N.D. Cal. May 27, 2016) (finding similar allegations "sufficient for purposes of pleading consequential injury at this point in litigation"). Therefore, the Court denies Defendant's Motion to dismiss Plaintiffs' negligence claims.

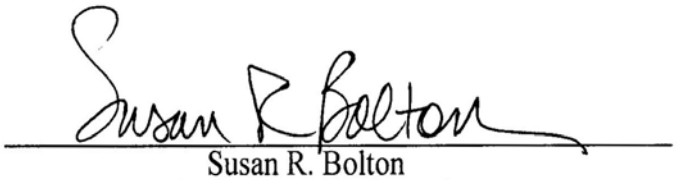
III. CONCLUSION

The Court grants in part Defendant's Motion to Dismiss because Plaintiffs have failed to allege adequately an enforceable express agreement between the parties providing for data security. This lack of an express agreement on the subject also precludes Plaintiffs' claims for breach of the implied covenant of good faith and fair dealing and the implied duty to perform with reasonable care. The Court denies in part Defendant's Motion because Plaintiffs have adequately alleged injury sufficient to support standing. They have also adequately pled their claims for unjust enrichment, a violation of the ACFA, and their negligence claims.

IT IS ORDERED granting in part and denying in part Defendant's Motion to Dismiss (Doc. 76).

IT IS ORDERED dismissing Plaintiffs' claims for breach of contract, breach of the implied covenant of good faith and fair dealing, and breach of the implied duty to perform.

Dated this 20th day of December, 2017.



Susan R. Bolton
United States District Judge