**NOT FOR PUBLICATION**

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

| | |
|---|---|
| Daniel Davila, individually and on behalf of all similarly situated persons,<br><br>Plaintiff,<br><br>v.<br><br>New Enchantment Group LLC,<br><br>Defendant. | No. CV-23-01098-PHX-SRB<br><br>**ORDER** |

The Court now considers Defendant New Enchantment Group LLC's ("Defendant") Motion to Dismiss Plaintiff Daniel Davila's ("Plaintiff") Complaint. (Doc. 10, Mot.)

## I. BACKGROUND

### A. Factual Background

This case arises out of a data breach that occurred in October 2022, when an unauthorized third party accessed Defendant's servers containing electronically stored personal identifying information ("PII"), such as names, social security numbers, driver's license numbers, and financial accounts; and protected health information ("PHI"), such as health insurance information ("Data Breach"). (Doc. 1, Compl. ¶¶ 2, 19, 22–23, 66.) On October 4, 2022, Defendant discovered that an unknown third party "accessed and acquired" electronically stored PII and PHI of its employees and customers from October 3, 2022, to October 4, 2022. (*Id.* ¶¶ 43–44, 47.)

Plaintiff is a former employee of Defendant and provided Defendant his PII and PHI "to receive employment and/or elective benefits." (*Id.* ¶ 76.) The purported class includes other employees and/or customers of Defendant for whom Defendant also collected and stored PII and PHI ("Class Members"). (*Id.* ¶¶ 1, 66.) According to Plaintiff, he provided Defendant with his PII and PHI with the understanding that Defendant would take adequate measures to protect this information. (*Id.* ¶ 71.) Around February 2023, Defendant began issuing letters notifying individuals whose PII and PHI had been compromised in the Data Breach ("Notice"). (*Id.* ¶ 47.) Between April 5 and May 4, 2023, Defendant learned that documents containing Plaintiff's name, social security number, and health insurance information had been compromised during the Data Breach and notified Plaintiff on June 6, 2023. (Compl. ¶¶ 47, 67, 78; *see* Doc. 1-2, Ex. 1, Notice of Data Breach at 1.) Defendant's Notice offered Plaintiff one free year of credit monitoring to "help[] detect possible misuse of . . . personal information." (Notice of Data Breach at 1.)

Plaintiff alleges that Defendant failed to properly secure and protect PII/PHI because Defendant, among other things, failed to monitor its systems for malware or unauthorized file access, failed to encrypt its servers and PII/PHI, did not train its employees on cybersecurity, and did not maintain "adequate computer systems and data security practices." (Compl. ¶¶ 26–33, 35–42, 106–07.) According to Plaintiff, Defendant's security protocols were inadequate because they did not meet the Federal Trade Commission's ("FTC") data security practices nor accepted industry standards. (*Id.* ¶¶ 58–65, 100–02.)

Plaintiff does not allege that he or any Class Member has yet experienced identity theft or fraud because of the Data Breach. (*See generally id.*) Instead, Plaintiff alleges that the third party responsible for the Data Breach intends to misuse the acquired PII/PHI, subjecting Plaintiff and Class Members to "a lifetime risk of identity theft." (*Id.* ¶¶ 48, 53, 57.) After receiving the Notice of the Data Breach, Plaintiff researched the Data Breach and reviewed his financial accounts. (*Id.* ¶ 79.) In addition to the "few hours" Plaintiff has expended on protecting himself from the Data Breach, Plaintiff expects to dedicate

"considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach." (*Id.* ¶¶ 80, 83.) Plaintiff alleges that the Data Breach and the prospect of identity theft or fraud has caused him emotional distress. (*Id.* ¶¶ 73, 82.)

**B. Procedural Background**

On June 14, 2023, Plaintiff brought this putative class action on behalf of himself and all Class Members who were notified that their PII and/or PHI had been compromised in the Data Breach. (*Id.* ¶¶ 44–46.) Plaintiff brings four causes of action against Defendant: Negligence (Count 1), Breach of Implied Contract (Count 2), Unjust Enrichment (Count 3), and Violations of the Arizona Consumer Fraud Act ("ACFA"), A.R.S. § 44-1521, *et seq.* (Count 4). (*Id.* ¶¶ 125–83.) Defendant filed the Motion on September 8, 2023. (*See* Mot.) Plaintiff filed his Response on September 27, 2023, to which Defendant replied. (Doc. 13, Resp. in Opp'n to Mot. ("Resp."); Doc. 14, Reply.) The Court heard oral argument on October 26, 2023. (*See* Doc. 18, Min. Entry.) Following oral argument, the parties each filed notices of supplemental authorities in support of their respective arguments. (Doc. 19, ("Def.'s Suppl. Authorities"); Doc. 20, ("Pl.'s Suppl. Authorities").)

## II. LEGAL STANDARDS & ANALYSIS

Defendant argues that Plaintiff lacks standing to bring his claims, and alternatively, that Plaintiff fails to state a claim under Rule 12(b)(6). (Mot. at 3–8.)

**A. Standing**

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). Plaintiff bears the burden of showing that he has standing. *Id.* at 561. In a class action, "[e]very class member must have Article III standing in order to recover individual damages." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021). A plaintiff must have standing for each claim and "for each form of relief that they seek." *Id.*

Defendant contends that Plaintiff has not alleged a concrete injury because he has not yet "suffered any form of identity fraud or other misuse" of PII/PHI and Plaintiff has not alleged a "certainly impending" threat of future harm as a result of the Data Breach. (Mot. at 1–4.) An injury is "concrete" if it "actually exist[s]" and is not merely "abstract." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016). The Supreme Court has specified that "intangible harms can . . . be concrete" and that "[c]hief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts," including "reputational harms, disclosure of private information, and intrusion upon seclusion." *TransUnion*, 594 U.S. at 425 (citing *Spokeo*, 578 U.S. at 340–41). While a plaintiff need not show "an exact duplicate," he must identify "a close historical or common-law analogue for [his] asserted injury." *Id.* at 424. In a suit for prospective injunctive relief, the risk of *future harm* may suffice for standing if "the risk of harm is sufficiently imminent and substantial." *Id.* at 435 (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). But in a suit for damages, "the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm." *Id.* at 436 (emphasis in original).

Plaintiff alleges sufficient facts to show standing to pursue injunctive relief and damages. First, Plaintiff alleges that his name and social security number were compromised during the Data Breach in "violation of his privacy rights." (Compl. ¶¶ 72, 78, 81; *see* Notice of Data Breach at 1.) The exposure of Plaintiff's PII/PHI is analogous to the common law harm of "disclosure of private information," which the Supreme Court has recognized as "one of many 'various intangible harms' that satisfy Article III standing."[1] *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 43 (D. Ariz. 2021) (citing

[1] The cases Defendant cites in support of its Motion are distinguishable. *See I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) (finding that the theft of "basic contact information" was "not analogous to the type of harm suffered as a result of [stolen] private information"); *In re Illuminate Educ. Data Security Incident Litig.*, No. SACV 22-1164 JVS (ADSx), 2023 WL 3158954, at *3 (C.D. Cal. Apr. 19, 2023) (ruling that plaintiffs failed to establish standing where plaintiffs had not alleged that social security numbers or financial information were stolen); (Def.'s Suppl. Authorities.)

*TransUnion*, 594 U.S. at 425); *see also Wynne v. Audi of Am.*, No. 21-cv-08518-DMR, 2022 WL 2916341, at *4 (N.D. Cal. Jul. 25, 2022) (ruling that "the 'invasion of [Wynne's] privacy interests' that occurred as a result of the theft of her PII, is a concrete injury that establishes Article III standing" (alteration in original)); *Bohnak v. Marsh & McLennan Cos., Inc.*, 79 F.4th 276, 285–86 (2d Cir. 2023) (ruling "disclosure of private information" "falls squarely within the scope of an intangible harm the Supreme Court has recognized as 'concrete'" in *TransUnion*).

Plaintiff also alleges facts to establish a sufficiently imminent and substantial risk of future harm. Plaintiff alleges that because the information compromised in the Data Breach will, among other things, allow criminals to open new financial accounts, obtain government benefits, and file fraudulent tax returns, Plaintiff "will continue to be at present, imminent, and continued increased risk of identity theft." (Compl. ¶¶ 8, 83.) According to Plaintiff, approximately one in four individuals notified of a data breach fall victim to identity fraud. (*Id.* ¶ 86.) Plaintiff also alleges that he spent "a few hours" researching the Data Breach and financial accounts after receiving the Notice of Data Breach and anticipates that he will need to expend "time and money on an ongoing basis" to protect himself from identity theft and fraud. (*Id.* ¶¶ 79–80, 83). Plaintiff has "suffered emotional distress as a result of the release of his Private Information" and has suffered "anxiety" about becoming a victim of identity theft or fraud following the Data Breach. (*Id.* ¶¶ 73, 82.) Plaintiff's mitigation efforts and emotional distress establish separate concrete harms resulting from "the sufficient likelihood of future identity theft" created by the exposure of Plaintiff's social security number and other personal information.[2] *Ortiz v. Perkins & Co.*, No. 22-cv-03506-KAW, 2022 WL 16637993, at *4 (N.D. Cal. Nov. 2, 2022) (ruling that while "the risk of increased future harm is not sufficient to establish standing" on its own, "the time spent dealing with the harm is a cognizable injury where,

[2] Defendant's contention that "Plaintiff has not alleged the theft of information which could immediately be used to commit fraud" is unpersuasive. (Mot. at 5.) Plaintiff specifically alleges that the Notice of Data Breach informed Plaintiff that his social security number and name had been compromised during the Data Breach. (Compl. 78; Notice of Data Breach at 1.)

as here, the information stolen could be used to commit identity theft"); *Whittum v. Univ. Med. Ctr. of Southern Nevada*, No. 2:21-cv-01777-MMD-EJY, 2023 WL 2967306, at *2 (D. Nev. Apr. 17, 2023) (ruling plaintiff had alleged separate concrete injuries where she alleged she spent time "investigating her financial accounts for evidence of fraud, and procuring her consumer disclosures from several credit reporting agencies" and "suffered stress, worry, anxiety, and hesitation from the feared risk of future fraud or theft"); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155–56 (3d Cir. 2022) ("[I]n the data breach context, where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms."); *see also TransUnion*, 594 U.S. at 436 n.7 (indicating that a plaintiff's knowledge that he is exposed to future monetary harm "could cause its own current emotional or psychological harm" but "tak[ing] no position" on how much or what type of emotional harm would suffice).

Defendant argues that Plaintiff's risk of future harm is speculative because Plaintiff has not identified "a single instance of identity fraud or other misuse of his personal information" because of the Data Breach. (Mot. at 3.) The court in *Ortiz v. Perkins & Co.* rejected a similar argument that a plaintiff could not conjure standing from fears of a hypothetical future harm. 2022 WL 16637993, at *4. There, the defendant had notified the plaintiff of a data breach, "offered complimentary credit monitoring and identity restoration," and recommended that the plaintiff monitor their accounts. *Id.* at *1. The court found that "[t]his is not a situation where . . . the chance of the stolen information being fraudulently used is so 'ephemeral' that it is merely speculative," as evidenced in part by the defendant's own recommendation that the plaintiff remain vigilant about her compromised information. *Id.* at *4–5. The court also cited *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692–94 (7th Cir. 2015), for the unremarkable proposition that the purpose of stealing private information is presumably "to make fraudulent charges or assume those consumers' identities." *Id.*; *see also Stallone v. Farmers Grp., Inc.*, No. 2:21-cv-01659-GMN-VCF, 2022 WL 10091489, at *5 (D. Nev. Oct. 15, 2022) (collecting cases

that infer malicious motives of thieves of personal identifying information). This reasoning applies here. Defendant acknowledged that Plaintiffs' PII/PHI was at risk and "encourage[d]" Plaintiff to "take advantage" of one free year of credit monitoring to protect himself from identity theft and fraud. (Compl. ¶ 49.)

Plaintiff alleges sufficient facts to establish standing for injunctive relief and damages.

**B. Failure to State a Claim**

A 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). 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.

**1. Breach of Implied Contract**

A valid contract requires an offer and acceptance, consideration, "sufficient specification of terms so that the obligations involved can be ascertained," and intent to be bound by the agreement. *Day v. LSI Corp.*, 174 F. Supp. 3d 1130, 1153 (D. Ariz. 2016), *aff'd*, 705 Fed. Appx. (9th Cir. 2017) (citations omitted). A contract may be implied in law or in fact. *Barmat v. John and Jane Doe Partners A-D*, 747 P.2d 1218, 1220 (Ariz. 1987)

(en banc). "A contract implied in fact is a true contract—an undertaking of contractual duty imposed 'by reason of a promissory expression'" via conduct. *Id.* (citation omitted). To state a claim for breach of an implied contract, a plaintiff must allege "the existence of the contract, its breach and the resulting damages." *Thomas v. Montelucia Villas, LLC*, 302 P.3d 617, 621 (Ariz. 2013) (en banc) (citation omitted).

**i. The Specific Terms of the Contract**

Defendant argues that Plaintiff fails to state a breach of implied contract claim because Plaintiff does not allege specific terms of the purported implied contract. (Mot. at 6.) "Contract terms cannot be vaguely pleaded. Even at the motion to dismiss stage, courts cannot be left to 'guess' how a party failed to perform their contractual obligations." *Griffey*, 562 F. Supp. 3d at 51 (citation omitted). According to Plaintiff, he and the Class Members entered implied contracts with Defendant, in which Defendant agreed to protect the Class Members' PII and PHI. (Compl. ¶ 145.) Specifically, Plaintiff alleges that as a condition of obtaining employment or services, he and Class Members were required to disclose their PII and PHI to Defendant. (*Id.* ¶ 146.) In return, Defendant made implied promises that it would:

> (1) tak[e] steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) tak[e] steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized purpose; (3) restrict[] access to qualified and trained agents; (4) design[] and implement[] appropriate retention policies to protect the information against criminal data breaches; (5) apply[] or requir[e] proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

(*Id.* ¶ 151.) Plaintiff and Class Members provided Defendant with their PII and PHI based on these assurances. (*Id.* ¶¶ 71, 152–53.) Plaintiff has alleged the specific terms of the implied contract. *Compare Castillo v. Seagate Tech., LLC*, No. 16-cv-01958-RS, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016) (ruling plaintiffs' allegations that the defendant "would take 'adequate measures' and make 'reasonable efforts' to 'properly safeguard' its employees personal identifying information" were sufficiently specific to state a claim), *with Griffey*, 562 F. Supp. 3d at 51 (granting motion to dismiss implied contract claim

where plaintiffs' conclusory allegations failed to describe the "applicability or scope" of the contract's terms). Furthermore, the Court agrees with those other courts that "it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of [sensitive personal information] would not imply the recipient's assent to protect the information sufficiently." *Castillo*, 2016 WL 9280242, at *9 (citation omitted).

**ii. Consideration**

Defendant also contends that Plaintiff's contract claim fails because "a promise to perform a pre-existing duty is insufficient consideration" and no implied contract can be formed without a promise beyond that legal duty. (Mot. at 6 (quoting *Hisel v. Upchurch*, 797 F. Supp. 1509, 1521 (D. Ariz. 1992))); *see Griffey*, 562 F. Supp. 3d at 52 ("[A] promise to perform a pre-existing duty is insufficient consideration." (citation omitted)). Plaintiff alleges that "industry standards, common law, state statutory law, and [Defendant's] own assurances and representations" imposed a duty on Defendant to protect Plaintiff's and Class Members PII. (Compl. ¶ 54.) Additionally, Defendant made "implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security," which went beyond existing duties under state and federal law. (Compl. ¶ 150.) This is sufficient to allege consideration under an implied contract for data security. *See Medoff v. Minka Lighting, LLC*, No. 2:22-cv-08885-SVW-PVC, 2023 WL 4291973, at *11 (C.D. Cal. May 8, 2023) ("Plaintiff is contending that the safeguard of data was an implied provision of the existing employment contract, which is supported by the consideration that he provided as part of his employment contract—his labor."); *Kirsten v. Cal. Pizza Kitchen, Inc.*, 2:21-cv-09578-DOC-KES, 2022 WL 16894503, at *5 (C.D. Cal. Jul. 29, 2022) (denying motion to dismiss implied contract claim where plaintiffs alleged that, as a condition of obtaining employment, plaintiffs "gave their PII to Defendant with the reasonable expectation that Defendant would protect their PII from a data breach" ).

Defendant's argument that Plaintiff fails to allege that Defendant promised to provide data security above that already legally required also fails because Defendant has

the burden of showing that Plaintiff fails to state a claim and "Defendant does not point to a particular statute that overlaps with Plaintiff's contract claim." (Mot. at 6); *Medoff*, 2023 WL 4291973, at *11 n.12 (citations omitted) (rejecting the defendant's pre-existing duty argument). In addition, Plaintiff's allegations are distinguishable from cases where this Court has determined a promise to protect PII was inadequate consideration to state a breach of implied contract claim.

The Plaintiffs in *In re Banner Health Data Breach Litigation*, alleged for example, that the defendant's privacy policy promised to safeguard personal information. No. CV-16-02696-PHX-SRB, 2017 WL 6763548, at *3 (D. Ariz. Dec. 20, 2017). The defendant's privacy policy stated the defendant was "committed to protecting the information *and* [was] required by law to do so," which this Court ruled "cannot be read as a promise to do anything above and beyond what is already required by law." *Id.* at *4 (citing to various regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")). Similarly, in *Griffey v. Magellan Health Inc.*, the defendant's privacy policy stated that the defendant used "physical, technical, and administrative safeguards to protect" private information and limited the information's use to providing service to the plaintiffs. 562 F. Supp. 3d at 52–53. This Court determined that plaintiffs' allegations that defendant "promised to comply with industry standards" was insufficient to allege that the defendant "promised to act beyond the existing HIPAA mandates." *Id.* at 52–53. Both *Banner Health* and *Griffey* are distinguishable, as those plaintiffs failed to allege promises beyond those contained in written privacy policies that confirmed the defendants' legal and regulatory requirements, such as HIPAA. Here, Plaintiff does not rely on a written policy but instead alleges that Defendant implicitly promised to protect PII/PHI by complying with industry standards that exceeded state and federal regulations. (Compl. ¶ 150.) The Court denies Defendant's Motion to dismiss Plaintiff's breach of implied contract claim.

**2. Unjust Enrichment**

"A claim for unjust enrichment may exist where a person confers a benefit to his detriment on another and allowing the other to retain that benefit would be unjust."

*Hannibal-Fisher v. Grand Canyon Univ.*, 523 F. Supp. 3d 1087, 1097 (D. Ariz. 2021) (citation omitted). To state a claim for unjust enrichment, a plaintiff must allege "(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."[3] *Griffey*, 562 F. Supp. 3d at 48 (quoting *Trustmark Ins. Co. v. Bank One, Ariz. NA*, 48 P.3d 485, 491 (Ariz. Ct. App. 2002)). Defendant contends that Plaintiff fails to sufficiently allege that Defendant was enriched or that Plaintiff was impoverished. (Mot. at 7.)

Plaintiff alleges he and Class Members either paid Defendant for services or provided labor that enabled Defendant to generate revenue and expected Defendant to allocate a portion of its revenue for data security. (Compl. ¶ 159.) Plaintiff further alleges that Defendant enriched itself by choosing not to spend its revenue on "a reasonable level of security" to protect Plaintiff's and the Class Members' PII/PHI. (*Id.* ¶ 160.) Courts have ruled that these types of cost-saving allegations are sufficient to state an unjust enrichment claim, as it would be "inequitable and unconscionable to permit" a defendant who receives the benefits of a plaintiff's data but does not "implement[] adequate safeguards" "to retain funds that it saved by shirking data-security and leaving the plaintiff to suffer the consequences."[4] *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1145 (C.D. Cal. 2021) (citation omitted) (ruling plaintiffs stated an unjust enrichment claim by alleging they paid defendants for services, expected a portion of payments would be used for data security, and defendants were enriched by not implementing adequate security measures to protect plaintiffs' information); *Banner Health*, 2017 WL 6763548, at *6 (ruling Plaintiffs stated a claim for unjust enrichment where plaintiffs "allege[d] that they

[3] Plaintiff may plead both breach of implied contract and unjust enrichment as alternative theories of relief. *Griffey*, 562 F. Supp. 3d at 48.

[4] Defendant contends that Plaintiff was not impoverished because Plaintiff does not allege that he paid for services or was not fairly compensated for his labor. (Mot. at 7.) The Court is unpersuaded by this argument. *See Griffey v. Magellan Health Inc.*, No. cv-20-01282-PHX-MTL, 2022 WL 1811165, at *6 (D. Ariz. June 2, 2022) (denying motion to dismiss where employee-plaintiffs alleged that their compensation packages included security measures to protect their data and defendant argued that plaintiffs were not impoverished because they "were paid for their services"); (Resp. at 11 n.4.)

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" (citing *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1200–01 (D. Or. 2016))); *see also Pyeatte v. Pyeatte*, 661 P.2d 196, 202 (Ariz. Ct. App. 1982) ("A benefit may be any type of advantage, including that which saves the recipient from any loss or expense.").

Defendant also argues that Plaintiff's allegation that Defendant did not provide a "reasonable level of security" does not describe how Defendant's security measures were inadequate. (Mot. at 7.) But Plaintiff specifically alleges that Defendant, among other things, failed to monitor its systems for malware, failed to encrypt PII/PHI, did not train employees on cybersecurity, and maintained former employees' personal information for longer than necessary. (Compl. ¶¶ 29, 32, 37, 42; *see* Resp. at 10.) Plaintiff's allegations are sufficient to state an unjust enrichment claim at the motion to dismiss stage.

**3. Arizona Consumer Fraud Act**

To state a claim under the ACFA, "a plaintiff must show (1) a false promise or misrepresentation made in connection with the sale or advertisement of 'merchandise,' and (2) consequent and proximate injury resulting from the misrepresentation." *Watts v. Medicis Pharmaceutical Corp.*, 365 P.3d 944, 953 (Ariz. 2016) (citing *Kuehn v. Stanley*, 91 P.3d 346, 351 (Ariz. Ct. App. 2004)). A claim under the ACFA based on an omission "requires proof that the omission is material and made with intent that a consumer rely" on the omission." *Cheatham v. ADT Corp.*, 161 F. Supp. 3d 815, 830 (D. Ariz. 2016) (quoting *State ex rel. Horne v. AutoZone, Inc.*, 275 P.3d 1278, 1281 (Ariz. 2012). Intent to deceive is not required for a plaintiff to state an ACFA claim. *Banner Health*, 2017 WL 6763548, at *7 (citing *Powers v. Guar. RV, Inc.*, 278 P.3d 333, 338 (Ariz. Ct. App. 2012)).

Defendant contends that Plaintiff does not plead his allegations of fraudulent misrepresentation with particularity as required under Rule 9(b). (Mot. at 8.) Specifically, Plaintiff does not specify "the documents, statements, or individuals alleged to be the source of [Defendant's] misrepresentation." (*Id.*) Defendant is correct that Rule 9(b)

applies to the ACFA. *See Lorona v. Ariz. Summit L. Sch., LLC*, 188 F. Supp. 3d 927, 935 (D. Ariz. 2016). But courts relax Rule 9(b)'s burden for plaintiffs alleging fraud-by-omission due to the "plaintiff's inherent inability to specify the time, place, and specific content of an omission in quite as precise a manner." *Griffey*, 562 F. Supp. 3d at 53–54. Plaintiff alleges that Defendant "omitted and concealed material facts, which it knew about and had the duty to disclose—namely, NEG's inadequate privacy and security protections for Plaintiff's and Class Members' Private Information. This omission was designed to mislead consumers." (Compl. ¶ 173; *see* Resp. at 12.) The Complaint provides several examples of these "inadequate" security protections. (*See* Compl. ¶¶ 29–32, 37–42, 64.) Plaintiff has adequately pleaded Defendant's omissions to state a claim under the ACFA. *See Cheatham*, 161 F. Supp. 3d at 831 (ruling the plaintiff stated an ACFA claim where the plaintiff alleged that the defendant "deliberately failed to disclose the fact that its wireless security system uses an unencrypted protocol and that this omission was material" and "designed to mislead customers").

The Court denies the Motion as to Plaintiff's ACFA claim.

## III. CONCLUSION

Plaintiff has standing because he has alleged sufficient facts to establish that he has suffered a concrete intangible injury because of the theft of his social security number and other personal identifying information. Plaintiff also alleges facts that a establish separate concrete injuries arising from his imminent and substantial risk of future harm. The Court denies Defendant's Motion to Dismiss the Complaint because Plaintiff alleges sufficient facts to state claims for breach of implied contract, unjust enrichment, and violations of the Arizona Consumer Fraud Act.

. . .

. . .

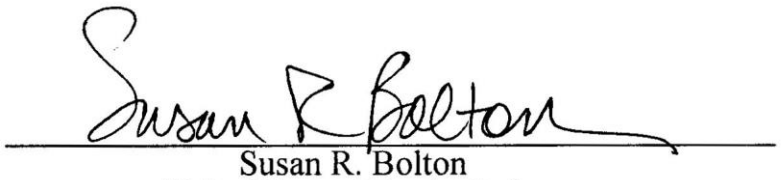
. . .

. . .

. . .

**IT IS ORDERED** denying Defendant New Enchantment Group, LLC's Motion to Dismiss (Doc. 10).

Dated this 25th day of April, 2024.



Susan R. Bolton
United States District Judge