IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
BALTIMORE DIVISION

RHONDA L. HUTTON, O.D. et al., Plaintiffs, v. NATIONAL BOARD OF EXAMINERS IN OPTOMETRY, INC. Defendant.	CASE NO. 1:16-CV-03025-JKB

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

This case arises from a data breach of the Defendant National Board of Examiners in Optometry ("NBEO")'s data systems, resulting in the misappropriation by fraudsters of thousands of optometrists' and optometry students' personal and financial information, including their names, dates of birth, Social Security numbers, addresses, and credit and/or debit card information (the "Personal Information"). Complaint ("Compl."), ¶ 2. The NBEO is the testing organization in the field of optometry in the United States of America (including Puerto Rico). The organization creates and administers various exams in the optometry profession. *Id.*, ¶¶ 1, 11. The NBEO requires exam-takers to provide their Personal Information to it as part of its exam administration process. *Id.*, ¶¶ 1-2, 12-13, 64. Plaintiffs Rhonda L. Hutton, O.D. and Tawny P. Kaeochinda, O.D. ("Plaintiffs") are optometrists who submitted their Personal Information to NBEO to register for required board-certifying exams eighteen and eight years ago, respectively, and whose Personal Information was stolen during the breach of NBEO's systems in July, resulting in Plaintiffs' identities being stolen by fraudsters. For both Plaintiffs, the Personal Information used to open fraudulent credit accounts was information provided to NBEO to register for its exams, but which is no longer current information for these Plaintiffs. *Id.*, ¶¶ 5-6.

Plaintiffs allege that NBEO's databases and lax data-security are the source and cause of optometrists' misappropriated Personal Information because the other optometry organizations with a relationship to optometrists nationwide neither gather nor store Social Security numbers and/or have investigated and confirmed that their databases have not been breached. *Id.*, ¶¶ 2, 16. Despite months passing and repeated contacts from scores of optometrists around the country informing NBEO that the information used to open fraudulent accounts in their names was information existing only in NBEO's systems, NBEO continues to refuse to accept responsibility

for its data breach, and has still not notified the thousands of affected individuals whose identities are being stolen without their knowledge. *Id.*, ¶¶ 19, 34, 48.

NBEO now moves to dismiss Plaintiffs' claims on the basis of lack of standing under Rule 12(b)(1) and for failure to state a claim under Rule 12(b)(6). NBEO also moves to strike Plaintiffs' class allegations and several important and relevant factual allegations. NBEO's motion must be denied in its entirety. Plaintiffs have alleged facts showing they have standing to sue because they have been injured, by, among other things, having their identities stolen, that the breach of NBEO's data systems was the cause of their injury, and that they have incurred monetary loss that is likely to be redressed by a judgment in their favor. Additionally, Plaintiffs have stated facts sufficient to show that NBEO is liable for negligence, breach of implied contract, breach of contract, and for violating California's Customer Records Act and Unfair Competition Law, requiring the denial of NBEO's 12(b)(6) motion. Finally, NBEO's motion to strike Plaintiffs' class allegations is premature, and its motion to strike several of Plaintiffs' substantive allegations going directly to the heart of Plaintiffs' claims is devoid of merit. NBEO's motion must be denied.

ARGUMENT

I. Plaintiffs have standing to sue because they have already suffered identity theft and fraud.

In order to establish standing to sue in federal court, the plaintiff "must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-561 (1992)). At the pleading stage, a plaintiff's burden to establish standing is simply to "'clearly . . . allege facts demonstrating' each element." *Id.* (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)).

A. Plaintiffs have alleged an injury in fact.

Plaintiffs must allege they have suffered an injury in fact that is concrete, particularized, and actual *or* imminent. *See Lujan*, 504 U.S. at 560-61. NBEO's entire argument contesting Plaintiffs' standing is premised on the idea that "apprehension of future injury" and "increased risk of identity theft" are insufficient to confer standing. Doc. 11-1 at 4-7. But this argument ignores Plaintiffs' allegations that they have *already experienced actual harm*. Thus, there is no need to speculate about the possibility or the likelihood of future injury in this case – Plaintiffs have already been the victims of identity theft and fraud linked to the NBEO breach. While Plaintiffs certainly remain at an imminent risk of future harm, they have alleged *actual* injuries that have *already* occurred. As discussed below, NBEO has not cited—and Plaintiffs are not aware of—any court opinion in the country holding that the injuries alleged by Plaintiffs do not constitute injury in fact.

1. The cases cited by NBEO are inapposite because they involve only speculative harm.

This Court recently reiterated the standard for establishing Article III standing in the context of a data breach case:

> [I]n the data breach context, plaintiffs have properly alleged an injury in fact arising from increased risk of identity theft if they put forth facts that provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud.

Khan v. Children's Nat'l Health Sys., No. CV TDC-15-2125, 2016 WL 2946165, at *5 (D. Md. May 19, 2016).

In *Khan*, the plaintiff asserted claims arising from a data breach whereby sensitive patient information was "potentially exposed" when hackers gained access to the email accounts of certain hospital employees. *Id.* at *1. There was no evidence, however, that the patients'

information had been misused or that the purpose of the hack was to obtain such data. *See id*. As a result, the court dismissed the case for lack of standing because the plaintiff failed to allege any "facts indicating that the hackers have attempted to engage in any misuse of [] patients' personal information since the breach was discovered." *Id*.

Here, by contrast, Plaintiffs have alleged both "actual examples" of the misuse of Plaintiffs' data and facts clearly indicating that the data was stolen for the purpose of committing identity theft and fraud. Plaintiffs allege that NBEO was the common source of fraud for a number of optometry students who had Chase Amazon Visa credit cards, or some other line of credit, fraudulently opened in their names. *See* Compl., ¶¶ 2, 15-17.[1] Both of the named Plaintiffs experienced fraud whereby unauthorized Chase Amazon Visa credit cards were opened in their names, using (now out-of-date) information that was provided to NBEO as part of the examination process. Plaintiffs allege that they spent time and money to address and mitigate this fraud, including putting credit freezes in place with the credit reporting agencies Experian, TransUnion, and Equifax, and filing reports with the FTC, FBI, IRS and local police departments. *See* Compl., ¶¶ 5-6. Under the standard set forth in *Khan*, Plaintiffs' allegations are clearly sufficient to confer Article III standing.

Curiously, NBEO fails to cite *Khan* despite its obvious relevance to the issues raised in NBEO's motion to dismiss. Instead, NBEO string cites inapposite data breach cases where the named plaintiff had not yet experienced identity theft and alleged *only* future harm as injury. But even those cases recognize that a plaintiff need not already have experienced harm as long as there are allegations supporting a realistic possibility of future misuse. For example, NBEO cites to *Chambliss v. Carefirst, Inc*, No. CV RDB-15-2288, 2016 WL 3055299, at *4 (D. Md. May 27,

[1] Since the filing of the Complaint, Plaintiffs' counsel has been contacted by dozens of optometrists who have experienced similar fraud traced to information provided to NBEO.

2016), where this Court dismissed a data breach case premised on the non-controversial principle that "the mere loss of data—*without any evidence that it has been either viewed or misused*—does not constitute an injury sufficient to confer standing." *Id*. at *4 (emphasis added). In *Chambliss*, the Court found that dismissal was appropriate because the type of information stolen was not conducive to fraud and there were no allegations of misuse:

> In this case, Plaintiffs do not allege that their data has been misused in any way thus far. The breach compromised only Plaintiffs' names, birthdates, email addresses, and subscriber identification numbers, and not their social security numbers, credit card information, or any other similarly sensitive data that could heighten the risk of harm. Plaintiffs contend that their personal information has value, but have not alleged how a hacker would use the particular information stolen to harm the Plaintiffs.

Id.

Again, this is in stark contrast to this case where Plaintiffs specifically allege that their stolen information includes Social Security numbers and *has already been used* to commit fraud.

The other cases cited by NBEO stand for the same proposition. *See In re Sci. Applications Int'l (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 19-20, 25 (D.D.C. 2014) (plaintiffs only alleging increased risk of identity theft had not established standing where stolen data tapes from car along with stereo and GPS system appeared to be the work of common criminal and tapes were not readable without specific hardware and software; however, plaintiffs claiming they had already suffered actual identity theft "clearly suffered an injury" to establish standing); *In re Zappos.com*, Civ. No. 12-cv-00325, 2016 WL 2637810, at *3-4 (D. Nev. May 6, 2016) (certain plaintiffs had not established standing where, three years after the data breach, they had not experienced an incident of fraud, demonstrating that the risk of harm was not imminent; however, plaintiffs that had experienced fraud had established standing); *see also In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 958 (D. Nev. 2015) (same); *Reilly v. Ceridian Corp*.,

664 F.3d 38, 45 (3d Cir. 2011) (plaintiffs had not established standing where they could point to no known instances of fraud or identity theft); *see also, e.g., Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) (complaint "provides no basis to believe that any of these events have come to pass or are imminent"); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *12 (N.D. Ill. Sept. 3, 2013) (plaintiffs "have not sufficiently alleged the information they are trying to protect was actually stolen").[2]

Simply put, none of the cases cited by NBEO are inconsistent with a finding of Article III standing in this case because in those cases the plaintiff was unable to satisfy the standard articulated in *Khan* by providing actual examples of identity theft or fraud or facts clearly indicating that the purpose of the data breach was to engage in identity fraud. *See Khan*, 2016 WL 2946165, at *5. Here, Plaintiffs allege actual instances of identity theft and fraud that have already occurred, as well as the loss of time and money mitigating their identity theft. These allegations are injuries in fact sufficient to confer Article III standing.

2. Plaintiffs' claim of standing is supported by cases across the country.

Even in cases where stolen information has not yet been misused, courts across the country have recognized that injuries like those alleged by Plaintiffs are sufficient to confer Article III standing. In *Galaria v. Nationwide Mutual Insurance Co.*, No. 15-3386, 2016 WL 4728027, at *3 (6th Cir. Sept. 12, 2016), the Sixth Circuit recently reversed a district court's dismissal of a data breach case in the context of a breach of Nationwide's computer network because the information was stolen for the purpose of committing fraud:

[2] NBEO's citation to *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014) should be disregarded because that holding was expressly overruled by the Sixth Circuit in *Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 WL 4728027, ---Fed. Appx.----, (6th Cir. Sept. 12, 2016).

> Plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation. Plaintiffs allege that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of "possible future injury" or "objectively reasonable likelihood" of injury that the Supreme Court has explained are insufficient. *Clapper*, 133 S. Ct. at 1147–48. 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.

Likewise, in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), the Seventh Circuit held that victims of a data breach at a department store had established injury-in-fact by alleging a "substantial risk of harm" from the theft of their data because: "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make a fraudulent charge or assume those consumers' identities." *Id*. at 693. Even absent existing fraud, the Seventh Circuit recognized that efforts taken by class members to mitigate future harm were sufficient to confer standing. *See id*. at 694 (purchasing credit monitoring costs "easily" qualified as Article III injury). The Seventh Circuit reached the same conclusion in *Lewert v. P.F. Chang's China Bistro, Inc*., 819 F.3d 963 (7th Cir. 2016), where restaurant customers' credit-card data was stolen in a data breach, because a "primary incentive" for a breach is to commit fraud. *Id*. at 965, 967. The Ninth Circuit similarly found Article III standing in *Krottner v. Starbucks Corp*., 628 F.3d 1139 (9th Cir. 2010), where employees brought suit after a thief stole a company laptop containing their personal information, concluding that plaintiffs had alleged facts showing a "credible threat of real and immediate harm." *Id*. at 1143.

District courts have made similar findings. In *In re Adobe Systems, Inc. Privacy Litigation*, hackers accessed the personal information of at least 38 million customers, including names, credit and debit card numbers, expiration dates and mailing and email addresses. 66 F.

Supp. 3d 1197, 1206 (N.D. Cal. 2014). The court found that "the threatened harm alleged [was] sufficiently concrete and imminent" because "the risk that Plaintiffs' personal data will be misused by the hackers . . . is immediate and very real." *Id.* at 1214. There, as here, speculation was not required as "stolen data had already surfaced on the internet." *Id.* at 1215. Accordingly "the danger that Plaintiffs' stolen data will be subject to misuse can plausibly be described as 'certainly impending'" and "the threatened injury here could be more imminent only if Plaintiffs could allege that their stolen personal information had already been misused." *Id*. *See also Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2015 WL 5793318, at *9 (M.D. Ala. Sept. 29, 2015) (finding that plaintiffs in a data breach case established injury in fact where they alleged identity theft and fraudulent tax returns were filed in their names); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016) (finding that plaintiffs' allegations of using their own time to monitor their credit in the aftermath of a data breach was injury in fact sufficient to confer standing).

Of course Plaintiffs' claim of standing is even stronger because their stolen information has already been misused. Thus, there "is no need for speculation" as to whether injury in this case is likely to occur. *Galaria*, 2016 WL 4728027, at *3. *See also In re Adobe*, 66 F. Supp. 3d at 1215. NBEO counters that *Neiman Marcus* and *P.F. Chang's* were "incorrectly decided" to the extent they diverge from the Supreme Court's holding in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013). Doc. 11-1 at 7. While NBEO's argument on this point is fuzzy at best, these decisions are not in any way inconsistent with the standard set forth in *Clapper*. In *Clapper*, the ACLU sought a declaratory judgment to halt new provisions of a federal statute that allowed the NSA to monitor certain communications. Notably, the ACLU filed suit before the challenged surveillance began. *Id.* at 1148. Unsurprisingly, the Supreme Court held that the plaintiffs lacked

standing to challenge the program because they "fail[ed] to offer any evidence that their communications have been monitored." *Id*.

Clapper did not represent a sea change in standing jurisprudence or immunize companies from liability for negligence. Rather, *Clapper* merely confirmed that where standing is based on a "threatened injury," that injury "must be *certainly impending* to constitute injury in fact" and "allegations of *possible* future injury are not sufficient." 133 S. Ct. at 1147 (citations omitted). In fact, *Clapper* endorsed finding standing "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." *Id.* at 1150 n.5 (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153 (2010)).

As noted by the Seventh Circuit, "[i]t is important not to overread *Clapper*." *Neiman Marcus*, 794 F.3d at 694. "*Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs. . . . An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring." *Id.*; *see also In re Adobe*, 66 F. Supp. 3d at 1214 ("Unlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both 'highly attenuated' and 'highly speculative,' the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real.") (citation omitted). The same is true here. Plaintiffs' information has *already* been misused and class members have *already* suffered concrete injuries, including actual financial consequences. Plaintiffs also face real, concrete and "certainly impending" continued threats stemming from the misuse of their Personal Information. These allegations easily satisfy Supreme Court jurisprudence regarding standing.

B. Plaintiffs' injuries are fairly traceable to NBEO's conduct.

To satisfy the "traceability" requirement, "there must be a causal connection between the injury and the conduct complained of," rather than the injury occurring as a result of "the independent action of some third party not before the court." *Daniels v. Arcade*, L.P., 477 Fed. Appx. 125, 129 (4th Cir. 2012) (quoting *Lujan*, 504 U.S. at 560) (citation omitted). "Traceability, however, does not require the defendant to be the only party responsible for the injury, or the party that contributes most significantly to the injury." *EarthReports, Inc. v. U.S. Army Corps of Engineers*, No. 8:10-CV-01834-AW, 2011 WL 4480105, at *6 (D. Md. Sept. 26, 2011) (citations omitted). The Fourth Circuit has stated that a plaintiff does not need to prove traceability with scientific certainty; rather, a plaintiff "'must merely show that a defendant discharges a pollutant that causes or contributes to the kinds of injuries alleged' in the specific geographic area of concern." *Id*. (quoting *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp*., 204 F.3d 149, 161 (4th Cir. 2000)).

In this case, Plaintiffs allege a clear causal link between their injuries and the NBEO breach. Both Plaintiffs allege that their fraud occurred using information that was stored by NBEO but that is no longer current. *See* Compl., ¶¶ 5-6. NBEO argues that there is "no factual basis" for the "conclusory and naked" assertion that NBEO suffered a data breach. Doc. 11-1 at 10. But at the pleading stage the allegations must be taken as true, and those allegations assert that thousands of optometrists have already experienced identity theft and fraud with the common source being NBEO. *See* Compl., ¶¶ 3, 16. Although NBEO continues to violate state statutes by failing to affirmatively notify affected optometrists, NBEO has tacitly acknowledged the breach occurred by issuing multiple statements that it is "investigating" the issue. *See id*., ¶ 4. Nothing further is required at this point to show that the harm is plausibly traceable to NBEO's misconduct. *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012) (holding

that allegations that laptops containing personal information were not adequately secured and then were stolen, and that plaintiffs thereafter experienced identity theft, satisfied Article III requirements).

NBEO also raises the factual issue that the "Chase Amazon Visa credit card scheme goes well beyond the optometry community." Doc. 11-1 at 11. This contention is not only an overt assertion of a purported "fact" not found within the four-corners of the Complaint, but it is also completely irrelevant. That fraudsters may have obtained the personal information of individuals not associated with NBEO to open fraudulent Chase Amazon Visa credit cards hardly renders implausible Plaintiffs' allegations that Chase Amazon Visa cards were opened using information obtained by fraudsters from NBEO's security-deficient data systems. As recognized in the pair of data breach decisions written by Judge Wood for the Seventh Circuit, the source or sources of harm present a question of fact—whereas the complaint's allegations must be accepted as true for purposes of Rule 12. Accordingly, "[m]erely identifying potential alternative causes does not defeat standing." *P.F. Chang's*, 819 F.3d at 969. *See also Neiman Marcus*, 794 F.3d at 696 ("The fact that Target or some other store might have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue. It is certainly plausible for pleading purposes that their injuries are 'fairly traceable' to the data breach at Neiman Marcus.").

NBEO's argument regarding the prevalence of data breach incidents assumes that individuals who reported past exposure to data breach incidents were not excluded from the group of potential class representatives. NBEO is not entitled to adverse inferences, and "[t]raceability does not require that the defendants be the only cause of the injury." *United States v. Ramos*, 695 F.3d 1035, 1046 (10th Cir. 2012). Indeed, courts have consistently rejected this same argument. In rejecting Anthem's argument that data breaches have become so prevalent as

to nullify the plaintiffs' traceability arguments, Judge Koh stressed: "the Court once again emphasizes: *no* court has ever accepted the Anthem Defendants' argument in the data breach context." *In re Anthem*, 2016 WL 3029783, at *16 (citing *Neiman Marcus*, 794 F.3d at 696). If accepted, NBEO's argument also would "create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable." *Id*. at *15. Plaintiffs have more than overcome the low burden of establishing traceability for standing purposes.

C. Plaintiffs' injuries will be redressed by an award of damages.

An injury is redressable if it is "likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *EarthReports*, 2011 WL 4480105, at *6 (quoting *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc*., 528 U.S. 167, 181 (2000)). Still, "no explicit guarantee of redress to a plaintiff is required to demonstrate a plaintiff's standing." *Id*. (quoting *Equity in Athletics, Inc. v. Dep't of Educ*., 639 F.3d 91, 100 (4th Cir. 2011)). Here, Plaintiffs have clearly alleged that they are the victims of identity theft and fraud and have and will continue to expend time and money in mitigation of that harm. *See* Compl., ¶¶ 30-35. Plaintiffs maintain, and NBEO does not contest, that an award of monetary damages may redress their injuries. Based on the foregoing, Plaintiffs have satisfied each element of Article III standing.

II. Plaintiffs have stated claims upon which relief can be granted.

On a motion to dismiss for failure to state a claim under Rule 12(b)(6), the court "must determine whether it is plausible that the factual allegations in the complaint are 'enough to raise a right to relief above the speculative level.'" *Monroe v. City of Charlottesville*, 579 F.3d 380, 386 (4th Cir. 2009) (quoting *Andrew v. Clark*, 561 F.3d 261, 266 (4th Cir. 2009)). "In doing so, the Court must examine the complaint as a whole, consider the factual allegations in the

complaint as true, and construe the factual allegations in the light most favorable to the plaintiff." *Young v. Swirsky*, No. CV GLR-14-3626, 2015 WL 6501164, at *3 (D. Md. Oct. 26, 2015) (citations omitted). Furthermore, "a court ordinarily may not consider matters that are outside the complaint or not expressly incorporated therein." *Id.*

A. Plaintiffs state valid claims for negligence.

NBEO argues that Plaintiffs have not stated two of the elements of a negligence claim – that NBEO owed a duty of care to the Plaintiffs and that Plaintiffs have sustained damages. NBEO does not dispute that, if it had a duty, Plaintiffs have sufficiently alleged NBEO breached that duty. Nor does NBEO challenge Plaintiffs' allegations that NBEO's breach was the proximate cause of Plaintiffs' injuries. *See Wagoner v. Dollar Gen. Corp.*, 955 F. Supp. 2d 1220, 1224 (D. Kan. 2013); *McIntyre v. Colonies-Pac., LLC*, 228 Cal. App. 4th 664, 671 (2014) (elements of negligence under California and Kansas law are the existence of a legal duty of care, breach of that duty, and that the breach proximately caused the plaintiff's injury).

Plaintiffs have sufficiently alleged that NBEO took on a duty to Plaintiffs when it collected, used and stored their highly sensitive Personal Information in its data systems as a precondition to allowing Plaintiffs to sit for required optometry board exams, to use reasonable care to ensure that Plaintiffs' Personal Information was secure. Additionally, Plaintiffs have alleged they have sustained damages in the form of having their identities stolen, the financial hardship of having to freeze and constantly monitor their credit for new fraudulent activity, and the certainly impending threat of future attempts by fraudsters to use Plaintiffs' Personal Information to obtain further unlawful benefits, including but not limited to additional lines of credit and fraudulent tax returns. NBEO's motion to dismiss Plaintiffs' negligence claims should denied.

1. Plaintiffs allege sufficient facts showing NBEO owed Plaintiffs a duty to exercise reasonable care.

NBEO – like every other person and legal entity – has a duty to exercise reasonable care when its action or inaction creates a risk of injury to others. As a part of its duty to exercise reasonable care when it collected, used and stored exam-takers' Personal Information, NBEO was obligated to undertake reasonable data security measures, consistent with industry standards, to protect that information from disclosure. Compl., ¶¶ 47-49. NBEO's only challenge to Plaintiffs' allegations of NBEO's duty of care is that Plaintiffs have not alleged a duty of care "recognized at common law." Doc. 11-1 at 13. While far from clear, NBEO appears to be arguing that because vast computer data systems containing the highly sensitive Personal Information of individuals, and the ability of criminals to hack into those systems to misappropriate that Personal Information, is a relatively new phenomenon, that no duty exists on the part of the entities that collect, use, and store that information as a condition of doing business to set up reasonable safeguards to ensure that Personal Information is protected. NBEO cites no authority for this implicit contention that a duty of care can only be recognized if the identical duty, defined narrowly, has been recognized for many years.

Of course, recent cases applying the common law to similar facts have recognized such a duty of care in this very context. *See, e.g.*, *In re Sony Gaming Networks and Customer Data Breach Security Litig*., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (holding "the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity . . . [is] well supported by both common sense and [applicable state] law"); *In re: The Home Depot, Inc., Customer Data Security Breach Litig*., No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016) ("A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused

foreseeable harm to a plaintiff and therefore owed a duty in tort."); *In re Target Corp. Customer Data Security Breach Litig*., 64 F. Supp. 3d 1304, 1308 (D. Minn. 2014) ("[G]eneral negligence law imposes a general duty of reasonable care when the defendant's own conduct creates a foreseeable risk of injury to a foreseeable plaintiff.") (citations omitted); *Resnick*, 693 F.3d at 1326-28 (finding health care provider had a duty to secure customers' information).

The authority cited by NBEO at pages 14 and 15 of its brief is distinguishable because in those cases the plaintiffs had no direct relationship with the defendants. In *Willingham v. Global Payments, Inc.*, No. 1:12–CV–01157–RWS, 2013 WL 440702 (N.D. Ga. Feb. 5, 2013), a magistrate judge recommended dismissing a negligence claim because the consumer plaintiffs sued a credit card processor—not a merchant—so there was "no direct relationship between the plaintiff and the defendant."[3] *Id.* at *18. The court explicitly distinguished the facts of *Willingham* from *Resnick*, *Claridge v. RockYou, Inc*., 785 F. Supp. 2d 855, 861 (N.D. Ca. 201l), and other cases where "the claimant had a direct relationship with the defendant and, therefore, had a basis for claiming that the defendant owed a duty of care." *Id.*; *see also In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1173 (D. Minn. 2014) (noting the distinction).

Likewise in *Worix v. MedAssets, Inc.*, 869 F. Supp. 2d 893 (N.D. Ill. 2012), the defendant was a "financial improvement partner for health care providers," and had no direct relationship with the plaintiff. *See Worix*, 857 F. Supp. 2d 699, 700 (N.D. Ill. 2012) (earlier opinion discussing facts); *see also Hammond v. The Bank of N.Y. Mellon Corp.*, No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *9 (S.D.N.Y. June 25, 2010) (concluding plaintiffs had alleged no duty of care because "[n]one of the named Plaintiffs had any direct dealings with Defendant," and "generally, banks owe no duty of care to their non-customers").

[3] *Willingham* has little persuasive value for the additional reason that the case was settled before the magistrate's recommendations were adopted or rejected by the district court.

Unlike these cases, NBEO had a direct relationship with its exam-takers and used their personal and financial information for its own benefit. In so doing, NBEO owed its exam-takers a duty of care to protect their information and to provide fair notice of a breach.

The reason NBEO's "no common law duty" argument fails is because the specific circumstances under which a person behaves unreasonably and causes foreseeable harm is not what determines whether the person has a duty of care. Rather, the fact that the person acted unreasonably and caused foreseeable harm is what results in the recognition of a duty of care. That is because "[e]veryone is under a general duty to exercise reasonable care under the circumstances to avoid injury to others." *Cardenas v. Kanco Hay, L.L.C.*, No. 14-1067-SAC, 2016 WL 3881345, at *3 (D. Kan. July 18, 2016) (citing *Striplin v. Kansas Gas & Electric Co*., 461 P.2d 825, 828 (Kan. 1969) and *Alford Ranches, LLC v. TGC Industries, Inc*., No. 112,375, 2015 WL 9591354, at *10-11 (Kan. Ct. App. Dec. 31, 2015)); *see also Alford Ranches*, 2015 WL 9591354, at *10 ("In general, anyone who does an affirmative act is under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act.") (citing Restatement (Second) of Torts § 302, Comment a (1965)); 57A Am. Jur. 2d Negligence § 88 ("[T]he law imposes upon every member of society the duty to refrain from conduct of a character likely to injure a person with whom he or she comes in contact and to use his or her own property in such manner as not to injure that of another."); Cal. Civ. Code § 1714 ("Everyone is responsible, not only for the result of his or her willful acts, but also for an injury occasioned to another by his or her want of ordinary care or skill in the management of his or her property or person."); *Rowland v. Christian*, 443 P.2d 561, 564 (Cal. 1968) ("All persons are required to use ordinary care to prevent others being injured as the result of their conduct."); *In re Syngenta AG MIR 162 Corn Litig.*, 131 F. Supp. 3d 1177, 1189 (D.

Kan. 2015) (finding close relationship between parties and the foreseeability of the harm established a duty of care).[4]

NBEO's contention that it owes no duty of care also implicitly appears to suggest that because fraudsters stole the Plaintiffs' Personal Information, that NBEO did not have a duty to use reasonable measures to prevent that information from falling into the hands of those fraudsters. *See* Doc. 11-1 at 14. That contention must be rejected because the fraudsters' actions were the foreseeable result of NBEO's negligent security practices. When "a criminal or intentional intervening act is foreseeable, or is part of the original risk negligently created by the defendant in the first place, then the harm is not outside the scope of the defendant's liability." Dan B. Dobbs et al., The Law of Torts § 209 (2d ed.). Thus, an actor remains liable if his negligence enabled a crime and "the actor at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime." Restatement (Second) of Torts § 448. *See also In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011) ("[Defendant] contends that the intervening acts of criminals broke the causal chain. . . . [¶] Because the security measures could have prevented the criminal acts committed by the skimmers, [defendant's] failure to implement such measures created a condition conducive to a

[4] Respectfully, the court in *Cooney v. Chicago Public Schools*, 943 N.E.2d 23, 28-29 (Ill. Ct. App. 2010), cited at page 14 of NBEO's brief, improperly failed to recognize, as NBEO does here, that "every person owes a duty of ordinary care to all others to guard against injuries which naturally flow as a reasonably probable and foreseeable consequence of an act." *Jane Doe–3 v. McLean Cnty. Unit Dist. No. 5 Bd. of Dirs.*, 973 N.E.2d 880, 887 (Ill. 2012). That oversight may have been the result of the plaintiffs' request in that case that the court "recognize a 'new common law duty' to safeguard information," *Cooney*, 943 N.E.2d at 28, rather than properly framing the issue as whether the defendant simply failed to exercise ordinary care to protect the plaintiffs from the foreseeable consequences of the defendant's failure to secure the plaintiffs' information. Likewise, the court in *Dolmage v. Combined Insurance Co. of America*, No. 14 C 3809, 2015 WL 292947, at *6 (N.D. Ill. Jan. 21, 2015), simply followed *Cooney* in concluding that "there is no common law duty to protect personal information in Illinois."

foreseeable intervening criminal act. Accordingly, the skimmers' reasonably foreseeable intervening criminal act did not sever the causal chain.").

Kansas and California law are also in accord on this point. *See Collins v. Navistar, Inc.*, 214 Cal. App. 4th 1486, 1504 (2013) ("[I]n some cases, intentional torts or criminal acts may be foreseeable and, therefore, within the scope of the risk defendant created, and in such a case the defendant may still be liable for the harm to the plaintiff resulting from the intentional or criminal act."); *cf. Storts v. Hardee's Food Sys., Inc.*, 210 F.3d 390, 2000 WL 358381, at *5 (10th Cir. 2000) (Kansas law "imposes on [defendants] a duty to provide reasonable and appropriate security if it is reasonably foreseeable, based on the totality of the circumstances, that 'its customers have a risk of peril above and beyond the ordinary.'") (quoting *Seibert v. Vic Regnier Builders, Inc.*, 856 P.2d 1332, 1338 (Kan. 1993)); *see also Nkemakolam v. St. John's Military Sch.*, 994 F. Supp. 2d 1193, 1198 (D. Kan. 2014) (applying § 448 of Restatement in rejecting the defendant's contention that an intervening criminal act broke the chain of causation where the defendant was alleged to have permitted the criminal act; citing *Citizens State Bank v. Martin*, 609 P.2d 670 (Kan. 1980)).

Additionally, even if a "special relationship" between NBEO and exam-takers is required to find a duty of care under Kansas law where NBEO created the hazard permitting criminals to infiltrate its systems and steal exam-takers' Personal Information,[5] Plaintiffs have alleged facts

[5] NBEO cites only one case for this proposition, and it was in the context of a claim brought by a minor-victim of sexual abuse against the wife of the assailant regarding abuse that occurred in the home of the wife and the assailant. The court held there was no special relationship between the wife and the minor, who was not a relative of the family, and who she had never invited into her home, such to impose a duty on her to warn the minor of her husband's propensities. *D.W. v. Bliss*, 112 P.3d 232, 240 (Kan. 2005). In this case, of course, NBEO did invite, in fact required, exam-takers to provide their Personal Information to NBEO to take required board-certifying exams. Therefore, this case is more analogous to the premises-liability cases in Kansas where courts do not require a "special relationship" between the business and its customers to impose a

sufficient to show that a special relationship exists between NBEO and the Plaintiffs. Plaintiffs have pled that optometry students are required to share their Personal Information, which includes dates of birth and Social Security numbers with NBEO as a condition of taking the optometry board exams necessary to practice optometry, and NBEO knew or should have known of the risk created by maintaining inadequate security, failed to take reasonable measures to protect that information, and failed to inform exam-takers that its data security systems would not stop hackers from obtaining their Personal Information, Compl., ¶¶ 2, 52. *See D.W. v. Bliss*, 112 P.3d 232, 238 (Kan. 2005) ("[A] special relationship or specific duty has been found when one creates a foreseeable peril, not readily discoverable, and fails to warn."). Thus, because a criminal data theft was a reasonably foreseeable consequence of deficient data security, Compl. ¶¶ 20-24, 53, NBEO had a duty to implement effective data security to protect against it.

NBEO's apparent contention that it has no duty whatsoever to protect the Personal Information of its exam-takers from disclosure should be a non-starter. NBEO cannot credibly argue that it would not be negligent for it to store such information in an open box in the lobby of its headquarters. Yet, under NBEO's logic, such action would not be negligent because it has no duty of care, regardless of the circumstances. Accepting NBEO's no-duty argument would weaken the incentives for companies to safeguard their customers' sensitive and financial information. As the court in *In re: Home Depot* stated, "[t]o hold that no such duty existed would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyber attacks, leaving consumers with no recourse to recover damages even though the retailer was in a superior position to safeguard the public from such a risk." 2016 WL 2897520, at *4.

---

duty of care to protect customers from the foreseeable criminal acts of third-parties. *See, e.g.*, *Storts*, 2000 WL 358381, at *5 (citing *Seibert*, 856 P.2d at 1338).

When NBEO took the affirmative act of collecting and storing exam-takers' names, addresses, dates of birth, Social Security numbers, and credit and debit card information, it owed those exam-takers a duty of care to protect that information from fraudsters. NBEO failed to act as a reasonable person when it did not enact reasonable data security safeguards for its exam-takers' Personal Information. The harm of a data breach is eminently foreseeable, as Plaintiffs' allegations regarding other recent data breaches in the industry and the likely result of having ones' personal information exposed to fraudsters show. Compl., ¶¶ 20-34. As such, Plaintiffs have established that NBEO had a duty to exercise reasonable care under the circumstances in collecting and storing Plaintiffs' Personal Information. Additionally, NBEO has not specifically challenged Plaintiffs' allegations that NBEO had a duty to timely notify exam-takers of the data breach (which NBEO still has not done) and to destroy exam-takers' information once it was no longer needed by NBEO. Compl., ¶¶ 48-49. These duties flow naturally from NBEO's duty to exercise reasonable care to protect exam-takers' information, and would have dramatically limited the overall harm caused by this data breach. Accordingly, the Court should readily conclude that Plaintiffs have alleged these additional duties of care as well.

2. Plaintiffs have pled present, actual injuries.

In asserting that Plaintiffs are unable to establish damages, NBEO merely rehashes its standing arguments. For the reasons discussed at Part I above, those arguments are unavailing and Plaintiffs have adequately alleged injury. Plaintiffs allege that they suffered identity theft and have spent time and money mitigating the effects of these identity thefts. Compl., ¶¶ 5-6, 58. These injuries have occurred; they are present and actual injuries. They are not speculative. NBEO's cases suggesting *merely* the fear of future harm is an insufficient injury to state a claim are simply not applicable here where Plaintiffs' identities were stolen and lines of credit were

opened using their Personal Information.[6] In addition, Plaintiffs allege that they face the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to their Personal Information being sold on the Internet black market and/or misused by criminals. *Id.* Likewise, these imminent injuries are actionable because they are injuries that are certain and continuing in nature.

3. The economic loss doctrine does not bar Plaintiffs' claims.

In one paragraph, NBEO argues that the economic loss rule bars Plaintiffs' claims for negligence. *See* Doc. 11-1 at 17. This rule seeks to ensure that tort law does not displace the enforcement of contracts; to this end, it "generally provides that a contracting party who suffers purely economic consequences must seek his remedy in contract and not in tort." *In re: Home Depot*, 2016 WL 2897520, at *3 (citation omitted). Despite NBEO's efforts to portray the economic loss rule as if it were absolute, it has "important limits" directly implicated here. Vincent R. Johnson, Cybersecurity, Identity Theft, and the Limits of Tort Liability, 57 S.C. L. Rev. 255, 302–03 (2005). The facts of this case—the nature of the services NBEO provided and the uniquely private information Plaintiffs disclosed—prevent application of the economic loss rule.

Most notably, NBEO forgets that under Kansas law where a duty arises independent of a contract, the economic loss rule does not bar a negligence claim. *See Rand Const. Co. v. Dearborn Mid-W. Conveyor Co.*, 944 F. Supp. 2d 1042, 1062 (D. Kan. 2013). Here, as discussed above, Plaintiffs have sufficiently alleged facts showing that NBEO had a duty to take

[6] Additionally, NBEO once again relies on a case that was reversed for its contention that Plaintiffs have not asserted actionable damages. *See Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164-65 (1st Cir. 2011) (reversing district court's conclusion that plaintiffs had not alleged actionable damages, holding even mitigation damages in the form of data theft protection were compensable injuries where there was wide-spread use by fraudsters of the stolen personal information).

reasonable measures to ensure Plaintiffs' Personal Information was secure, and this duty arises from the common law, not only from contract. Likewise, California recognizes a special relationship exception to the economic loss rule that precludes application of the economic loss doctrine in this case. *See J'Aire Corp. v. Gregory*, 598 P.2d 60, 62-63 (Cal. 1979). The factors considered include: (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. *Id.* at 63. All six factors must be considered by the court and the presence or absence of one factor is not decisive. *See Kalitta Air, LLC v. Cent. Tex. Airborne Sys., Inc.*, 315 Fed. Appx. 603, 605-06 (9th Cir. 2008).

In this case, each factor is satisfied. Plaintiffs allege that the parties had a "special relationship," Compl., ¶ 52, because: (1) NBEO required Plaintiffs to share their Personal Information with NBEO as a condition of taking the optometry board exams necessary to practice optometry, *id.* at ¶ 52, and thus, NBEO's conduct as it related to Plaintiffs' Personal Information was directly intended to affect Plaintiffs, and Plaintiffs would not have provided NBEO with their Personal Information had Plaintiffs known that NBEO's security practices were deficient, *id.*, ¶ 75; (2) the harm resulting from NBEO's failure to secure Plaintiffs' Personal Information was foreseeable, *id.*, ¶¶ 20-34, 53; (3) Plaintiffs suffered injuries, *id.*, ¶¶ 5-6, 25-34, 58, 67; (4) Plaintiffs' injuries flowed directly from the breach, *id.*, ¶¶ 34, 58; (5) NBEO's degree of negligence is severe and there is a strong moral blame attached to its conduct, *id.*, ¶ 51; and (6) there is a strong public policy to protect customers' personal and financial information, *id.*, ¶ 52. Thus, California would recognize an exception to the economic loss doctrine under the facts

alleged in this case. Furthermore, where NBEO denies the existence of a contract, *see* Doc. 11-1 at 18-20, it should not be heard to argue that recovery is unavailable in tort law.

B. Plaintiffs state valid claims for breach of contract.

Plaintiffs allege that NBEO promised in its Privacy Statement that it had implemented important security measures to protect exam-takers' Personal Information. Compl., ¶ 64, and that this promise, which Plaintiffs accepted by handing over their Personal Information, created an enforceable contract between Plaintiffs and NBEO. *Id.* ¶ 65. NBEO violated that Privacy Statement, and breached its contract, by (1) failing to implement security measures designed to prevent this attack, (2) failing to employ security protocols to detect the unauthorized network activity, and (3) failing to maintain basic security measures such as complex data encryption so that if data were accessed or stolen it would be unreadable, *id.*, ¶ 66, thereby exposing Plaintiffs' information to hackers and causing Plaintiffs to incur damages, *id.*, ¶¶ 5-6, 67.

NBEO's perfunctory challenge to Plaintiffs' breach of contract claim, on the unadorned ground that the parties failed to reach a meeting of the minds on all essential terms of the contract, should be rejected. Doc. 11-1 at 18. NBEO does not explain what term is missing from the agreement or how one party to it had a different understanding of its meaning. NBEO's promises as to the security measures it had implemented are clear and created a unilateral contract, whereby Plaintiffs' handing over of their Personal Information constituted acceptance of NBEO's offer to implement the security measures promised. *See Smith v. Kansas Orthopaedic Ctr., P.A.*, 316 P.3d 790, 795 (Kan. Ct. App. 2013) ("In a unilateral contract, one party makes a promise in exchange for the other party's performance rather than a corresponding promise."); *Sateriale v. R.J. Reynolds Tobacco Co.*, 697 F.3d 777, 785 (9th Cir. 2012) ("[A] unilateral contract involves the exchange of a promise for a performance. The offer is accepted by rendering a performance rather than providing a promise.") (internal citations omitted).

NBEO's efforts to downplay and, indeed, to ignore, its Privacy Statement as the contractual predicate fail categorically, for courts have found that performance undertaken with the understanding that private information would be protected in accordance with such a privacy statement gives rise to a unilateral contract. Three cases are especially noteworthy. In *Meyer v. Christie*, where the court allowed a breach of contract claim to proceed, the court rejected the defendant's "attempt to characterize its privacy policy as nothing more than a mere unilateral statement of company policy," concluding that the plaintiff had "divulged information to the bank with the understanding that the bank would keep it confidential in accordance with its privacy policy." No. 07-2230-JWL, 2007 WL 3120695, at *4 (D. Kan. Oct. 24, 2007). In the *In re Jetblue Airways Corporation Privacy Litigation*, the court upheld the plaintiffs' allegations "that a stand-alone contract was formed at the moment they made flight reservations in reliance on express promises contained in [defendant's] privacy policy." 379 F. Supp. 2d 299, 325 (E.D.N.Y. 2005). And most recently, the court in *Enslin v. The Coca-Cola Company* allowed a breach of contract claim to proceed where the defendant, "through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard [plaintiff's data] in exchange for his employment." 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015).

The cases cited by NBEO are distinguishable. In *Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196 (D.N.D. 2004), the court rejected claims for breach of contract against an airline pursuant to its privacy policy after the airline shared passenger data with the United States government, concluding that "broad statements of company policy do not generally give rise to contract claims." *Id.* at 1200; *see also In re Nw. Airlines Privacy Litig.*, No. CIV.04-126, 2004 WL 1278459, at *5 (D. Minn. June 6, 2004) (same). Here, Plaintiffs have alleged specific promises made by NBEO in its Privacy Statement stating what it would do to protect exam-

takers' Personal Information. The court in *Meyer v. Christie*, *supra*, cited and specifically rejected the rationale in *Dyer* and *In re Nw. Airlines*, especially at the pleading stage:

> [On a motion to dismiss], the court cannot agree with the bank's attempt to characterize its privacy policy as nothing more than a mere unilateral statement of company policy. Plaintiffs' complaint alleges that Mr. Meyer had a long-term banking business and banking relationship with Security Savings; that in the course of that relationship he relied on the bank to preserve his confidential information according to the terms of its privacy policy; and that the bank had solicited his financial information when it requested that he act as a personal guarantor on the loans that it made to ERP. Inferentially, then, the bank's privacy policy was part and parcel of its offer to make the loan to ERP, which was accepted when Mr. Meyer divulged information to the bank with the understanding that the bank would keep it confidential in accordance with its privacy policy. Under this view of the facts, the bank's privacy policy constituted part of Mr. Meyer's bargained-for exchange with the bank.

2007 WL 3120695, at *4.

Plaintiffs have similarly alleged a long-term relationship with NBEO, both having submitted their Personal Information to NBEO years ago. Compl., ¶¶ 5-6. Likewise, Plaintiffs allege they submitted their Personal Information to NBEO with the understanding that their Personal Information would be protected in accordance with NBEO's Privacy Statement, and that NBEO invited and required Plaintiffs to submit their Personal Information to register for board-certifying exams. *Id.*, ¶¶ 52, 64-65. Thus, this Court can infer, as the *Meyer* court did, that NBEO's Privacy Statement was "part and parcel of its offer" to register Plaintiffs for their exams, which was accepted when Plaintiffs divulged information to NBEO with the understanding that NBEO would protect that information in accordance with its Privacy Statement. *See* 2007 WL 3120695, at *4. Therefore, NBEO's Privacy Statement "constituted part of [Plaintiffs'] bargained-for exchange with [NBEO]." *Id.* As to NBEO's contention that Plaintiffs have not alleged a cognizable injury, Plaintiffs refer the Court to their standing discussion above, *supra*, Part I.

C. Plaintiffs have stated valid claims for breach of implied contract.

NBEO solicited, invited, and required exam-takers to hand-over their Personal Information to NBEO to take required board examinations. *See* Compl., ¶ 72. Implicit in this requirement was a promise to adequately safeguard Plaintiffs' Personal Information and to timely notify them of any breach. *See id*., ¶¶ 69-78. Plaintiffs accepted NBEO's offers by providing their Personal Information to register and pay for board exams. *See id*., ¶ 72. NBEO breached its implied contracts and Plaintiffs suffered losses as a result. *See id*., ¶¶ 77-78.

NBEO argues Plaintiffs have failed to allege intent on the part of NBEO to enter into a contract or a "meeting of the minds" to enter into an implied contract for the protection of Plaintiffs' Personal Information. *See* Doc. 11-1 at 19-20. Courts have consistently rejected this argument in data breach cases, finding that "a determination of the terms of [the] alleged implied contract is a factual question that a jury must determine." *Target*, 66 F. Supp. 3d at 1176-77 (citing *In re Hannaford Bros. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 118-119 (D. Me. 2009) (jury issue) and *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011) (same)); *In re Michaels Stores Pin Pad Litig*., 830 F. Supp. 2d at 528 (retail transaction created "an implicit contractual relationship between Plaintiffs and Michaels, which obligated Michaels to take reasonable measures to protect Plaintiff's financial information and notify Plaintiffs of a security breach within a reasonable amount of time."). As to NBEO's contention that Plaintiffs have not alleged a cognizable injury, Plaintiffs refer the Court to their standing discussion above, *supra*, Part I.

D. Plaintiff Kaeochinda states a claim under the California Customer Records Act.[7]

Plaintiff Kaeochinda alleges NBEO violated three provisions of the California Customer Records Act (CRA). First, NBEO violated section 1798.81.5, Compl., ¶¶ 81-85, which states that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5. Second, Plaintiff Kaeochinda alleges that NBEO's unreasonable retention of exam-takers' Personal Information long after the need to retain the information had ceased violated section 1798.81, Compl., ¶¶ 2, 6, 86, which requires businesses to dispose of records containing Personal Information "when the records are no longer to be retained by the business." § 1798.81. Third, Plaintiff Kaeochinda alleges that NBEO violated section 1798.82 by failing to promptly notify affected NBEO exam-takers that their Personal Information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach. Compl., ¶¶ 18-19, 87.

NBEO first challenges Plaintiff Kaeochinda's statutory standing to make a claim under the CRA, contending she has not alleged a cognizable injury traceable to NBEO's conduct. Again, Plaintiffs refer the Court to their standing discussion above, *supra*, Part I.[8] NBEO is also incorrect that Plaintiffs have not alleged any injury from NBEO's delay in notifying exam-takers

[7] Counts IV and V are brought by Plaintiff Kaeochinda, a resident of California, on behalf of herself and the California Subclass.

[8] NBEO's contention that the "Chase Amazon Visa credit card scheme has affected individuals outside the optometry community that have no relation whatsoever to Defendant," Doc. 11-1 at 21, is once again not only an assertion of a purported "fact" not found in the Complaint, but it is also completely irrelevant. That fraudsters may have obtained the personal information of individuals not associated with NBEO to open fraudulent Chase Amazon Visa credit cards hardly casts doubt on Plaintiffs' claim that fraudsters used the Personal Information of numerous individuals obtained from NBEO's data systems to do so.

of the breach. Had NBEO notified exam-takers immediately upon discovering the breach (which if not discovered in a timely manner was due to NBEO's failure to properly monitor its systems to identify suspicious activity), Compl., ¶ 54, Plaintiffs would have been able set up credit monitoring and/or credit-freezes *before* fraudulent accounts were opened in their names. *See, e.g.*, Compl., ¶¶ 19, 56.

Next, NBEO challenges Plaintiff Kaoechinda's claim under section 1798.81 that NBEO failed to take all reasonable steps to dispose, or arrange for the disposal, of exam-takers' records within its custody or control containing Personal Information when the records should no longer have been retained by NBEO. Compl., ¶ 86. Section 1798.81 provides as follows:

> A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information *when the records are no longer to be retained by the business* by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

Cal. Civ. Code § 1798.81 (emphasis added).

In particular, Plaintiff Kaeochinda's allegations are related to the fact that NBEO continues to store the Personal Information of exam-takers who took its exams years ago, well after the registration and exam administration process was over and NBEO's need for the Personal Information had ended. *See id.* at ¶¶ 2, 5-6. Had NBEO properly disposed of exam-takers' Personal Information within a reasonable time after the exam-administration process was complete, many people that have been affected by this data breach would have been spared the misery it has caused, including Plaintiff Kaeochinda, who took NBEO's exams eight years ago. *See id.* at ¶ 6; *see also id.* at ¶ 2. While Section 1798.81 is largely untested, two cases, apparently the only two cases that have interpreted the statute, have concluded that it "applies only to situations where a business intends to discard records containing personal information." *Frezza*

v. Google Inc., No. 12-CV-00237-RMW, 2012 WL 5877587, at *5 (N.D. Cal. Nov. 20, 2012) (citing *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1114 (N.D. Cal. 2010)). That interpretation simply does not square with the plain language of the statute stating businesses must properly discard personal information "when the records are no longer to be retained by the business." § 1798.81. Plaintiff Kaeochinda alleges her Personal Information was "no longer to be retained by" NBEO because its need to retain it had long-ended. The *Frezza* and *Doe 1* courts' interpretation of section 1798.81 does not meet the stated objectives of the Act, which is to "ensure that personal information about California residents is protected." *Id.* at § 1798.81.5. Recognizing Plaintiff Kaeochinda's claim under § 1798.81 here would meet that objective, and the statute should be interpreted accordingly. In addition, discovery may yet reveal that NBEO intended to discard the data, so it is plausible that Plaintiffs will meet even the restrictive view of the statute as interpreted in *Frezza* and *Doe 1*.

Thus, NBEO's motion to dismiss Plaintiff Kaeochinda's CRA claim is without merit and should be denied in its entirety.[9]

E. Plaintiff Kaeochinda states a claim under the UCL.

California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair or fraudulent act." Cal. Bus. & Prof. Code § 17200. "Its coverage is sweeping." *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 973 P.2d 527, 539 (Cal. 1999) (internal quotations omitted). "The unlawful prong of the UCL prohibits anything that can properly be called a business practice and that at the same time is forbidden by law." *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 989 (N.D. Cal. 2016); *In re Adobe*, 66 F. Supp. 3d at 1225. "Generally, violation of almost any law may serve as a basis for a UCL claim." *In re Anthem,*

[9] Plaintiff Kaeochinda does not request statutory damages pursuant to § 1798.84(c), as she does not allege a violation of § 1798.83.

162 F. Supp. 3d at 989. NBEO contends Plaintiff Kaeochinda has not pled the violation of another law; however, because NBEO's challenges to Plaintiff's CRA claim fail, her UCL claim premised on the violation of the CRA states a claim. Under similar data breach allegations, the court in *In re Anthem* concluded the plaintiffs had stated a claim under the UCL's unlawful prong by alleging the defendant had violated the CRA, among other statutes. *Id.* at 989.

As to Plaintiff Kaeochinda's "unfair" claims, NBEO rehashes the same arguments it made challenging standing, contending Plaintiffs' allegations that NBEO was the source of the data breach are speculative, and that NBEO should be relieved of liability because "a third-party criminal accessed Plaintiffs' information, not the Defendant." Doc. 11-1 at 25. Plaintiff incorporates her arguments as to Plaintiffs' standing, *see* Part I. Additionally, Plaintiff does not assert that NBEO should be held liable for "access[ing] Plaintiffs' information." Rather, Plaintiff Kaeochinda's UCL unfairness claim is premised on NBEO's failure to maintain adequate and reasonable security measures to protect exam-takers' Personal Information from third-party criminals, and in unduly delaying informing them of the data breach. Both of these failures undermine or violate California public policy and therefore state a claim under the UCL's unfair prong. *In re Anthem,* 162 F. Supp. 3d at 990; *In re Adobe,* 66 F. Supp. 3d at 1227; *In re: Home Depot,* 2016 WL 2897520, at *6.

Finally, NBEO contends Plaintiff Kaeochinda's UCL claim fails because Plaintiffs have not lost money or property as a result of the alleged unfair competition. Doc. 11-1 at 25. To have statutory standing under the UCL, a plaintiff must demonstrate injury in fact and a loss of money or property caused by the unfair competition. *In re Anthem*, 162 F. Supp. 3d at 985. "There are innumerable ways in which economic injury from unfair competition may be shown." *Kwikset Corp. v. Superior Court*, 246 P.3d 877, 885 (Cal. 2011). "A plaintiff may, for instance, (1)

surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." *Id.* at 885-86.

Here, Plaintiffs allege that when they provided their Personal Information to NBEO for purposes of exam-administration, they believed that its data security practices and policies were state-of-the-art and that it would use part of the cost for the exam that exam-takers pay for such state-of-the-art practices. Exam-takers thus entered into an implied contract with NBEO that NBEO would adequately secure and protect their Personal Information, and would use part of the price for its services to pay for adequate data security measures. In fact, rather than use those moneys to implement adequate data security policies and procedures, NBEO failed to provide reasonable security measures. Compl., ¶ 71. Plaintiffs further allege that they lost the value of their Personal Information and have paid money to monitor their credit to help protect themselves from further instances of identity theft. Compl., ¶¶ 5-6, 67. Thus, at the very least, Plaintiffs have "acquired in [the] transaction" with NBEO "less than [they] otherwise would have," have had a "present or future property interest diminished," and were "required to enter into a transaction, costing money . . . that would otherwise have been unnecessary." *Kwikset*, 246 P.3d at 885-86; *see also In re Anthem*, 162 F. Supp. 3d at 985 (canvassing recent case law and concluding that the plaintiffs' allegations that they had received less in their transaction with the defendant than they otherwise would have if defendant had spent money to implement reasonable security measures to protect the plaintiffs' personal information, satisfied the lost money or property requirement for standing under the UCL).

As to Plaintiff Kaeochinda's recovery under the UCL, prevailing plaintiffs in UCL actions are entitled to injunctive relief and restitution, including restitutionary disgorgement. *Cel-Tech*, 973 P.2d at 539; *Madrid v. Perot Sys. Corp.*, 130 Cal. App. 4th 440, 460 (2005); *see also In re Anthem*, 162 F. Supp. 3d at 986. Thus, if she prevails, Plaintiff Kaeochinda will be entitled to an injunction as set forth in paragraph 102 of the Complaint, as well as a return of all money NBEO obtained from the California Class that should have been used by NBEO to ensure that its data security was sufficient to protect class members' Personal Information. *See In re Anthem*, 162 F. Supp. 3d at 986 (where plaintiffs alleged defendant profited from its lax security measures because plaintiffs overpaid for defendant's product based on the assumption that some portion of their payments would go toward reasonable data security measures, plaintiffs' request for unfairly obtained profits was recoverable as restitution). Contrary to NBEO's assumptions, Plaintiff Kaeochinda and the California Subclass do not seek to recover the amounts paid for identity theft protection through their UCL claim.

III. NBEO's motion to strike class allegations is premature and groundless.

NBEO next moves to strike the Complaint's class allegations. *See* Doc. 11-1 at 27-30. NBEO's motion is premature as the breach of NBEO's database was only discovered in late July of this year, the Complaint was filed just over two months ago on August 30, 2016, and Plaintiffs have been provided no opportunity to request or obtain any discovery whatsoever, including the results of NBEO's purportedly ongoing investigation into the matter. Numerous courts have rejected motions to strike class allegations made before briefing on class certification, let alone before discovery has gotten underway.[10] *See, e.g., Goodman v. Schlesinger*, 584 F.2d 1325, 1332

[10] NBEO's rationale for striking the class allegations now is in part that the Federal Rules "allow a court to determine the issue of class certification at an 'early practicable time.'" Doc. 11-1 at 27 (quoting Fed. R. Civ. P. 23(c)(1)(A)). But this language superseded the prior "as soon as practicable after the commencement of the action" because "[t]he 'as soon as practicable'

(4th Cir. 1978) (district court improperly dismissed class allegations prematurely when discovery had not occurred and the factual record was incomplete); *Doctor v. Seaboard C. L. R. Co.*, 540 F.2d 699, 707 (4th Cir. 1976) (class certification determination "usually should be predicated on more information than the complaint itself affords") (internal quotations omitted); *Law Offices of Leonard I. Desser, P.C. v. Shamrock Commc'ns, Inc.*, No. 1:12-cv-02600-JKB, ECF Doc. 37 at 4 (D. Md. May 21, 2013) ("This motion [to strike] is effectively an opposition to Plaintiff's anticipated motion for class certification and is premature.") (citing *See* 7B Charles A. Wright, Arthur R. Miller, & Mary Kay Kane, *Federal Practice & Procedure* § 1795, at 40 (3d ed. 2005)); *Jarboe v. Md. Dep't of Pub. Safety & Corr. Servs. (DPSCS)*, No. 1:12-cv-00572-ELH, ECF Doc. 49 at 27 (D. Md. Mar. 13, 2013) ("[Defendants'] challenge to the suitability of this case for class treatment is premature, because no motion for class certification is pending before the Court.").[11] Thus, NBEO's motion to strike Plaintiffs' class allegations is premature and must be denied.[12]

---

exaction neither reflects prevailing practice nor captures the many valid reasons that may justify deferring the initial certification decision." Committee Notes to the Rule's 2003 Amendment (citations omitted). In other words, the language of the rule is not a command to courts to rush breakneck into a determination about class certification prior to allowing parties to gather and provide to the Court "information necessary to make the certification decision," *i.e.*, class certification discovery. *See, e.g., Barghout v. Bayer Healthcare Pharm.*, No. 11-CV-1576 DMC JAD, 2012 WL 1113973, at *11 (D.N.J. Mar. 30, 2012), at *30 ("Legislative history tells us that the Advisory Committee commented upon this change as reflecting the time that 'may be needed to gather information necessary to make the certification decision.' Such 'information,' the Committee explained further, included discovery and that 'required to identify the nature of the issues that actually will be presented at trial.'") (quoting Fed. R. Civ. P. 23 advisory committee's note).

[11] *See also, e.g., Bryant v. Food Lion, Inc.*, 774 F. Supp. 1484, 1495 (D.S.C. 1991); *Barghout*, 2012 WL 1113973, at *9; *Chenensky v. New York Life Ins. Co.*, No. 1:07-cv-11504-WHP-JLC, ECF Doc. 71 at 3 (S.D.N.Y. Apr. 27, 2011); *Beauperthuy v. 24 Hour Fitness USA, Inc.*, No. 06-0715 SC, 2006 WL 3422198, at *3 (N.D. Cal. Nov. 28, 2006); *Cholakyan v. Mercedes-Benz USA, LLC*, 796 F. Supp. 2d 1220, 1245-46 (C.D. Cal. 2011); *Boatwright v. Walgreen Co.*, No. 10 C 3902, 2011 WL 843898, at *2 (N.D. Ill. Mar. 4, 2011); *In re Wal-Mart Stores, Inc. Wage and Hour Litig.*, 505 F. Supp. 2d 609, 616 (N.D. Cal. 2007); *Myers v. MedQuist, Inc.*, No. CIV

IV. NBEO's motion to strike certain factual allegations should be denied.

NBEO also contends that several allegations in the Complaint it deems "immaterial, impertinent and scandalous" should be stricken pursuant to Fed. R. Civ. P 12(f). Doc. 11-1 at 31. Rule 12(f) states that "the court may order stricken from any pleading any insufficient defense or any redundant, immaterial, impertinent or scandalous matters." However, "Rule 12(f) motions are generally viewed with disfavor because striking a portion of a pleading is a drastic remedy and because it is often sought by the movant simply as a dilatory tactic." *Waste Mgmt. Holdings v. Gilmore*, 252 F.3d 316, 347 (4th Cir. 2001). NBEO concedes that an allegation must be "both immaterial and prejudicial" in order to be stricken. Doc. 11-1 at 31.[13] Moreover, for an allegation

---

05-4608 JBS, 2006 WL 3751210, at *5 (D.N.J. Dec. 20, 2006); Charles Alan Wright, Arthur R. Miller & Mary Kay Kane, *Federal Practice and Procedure* § 1785.3 (3d ed. 2009) (all stating pre-discovery motion to strike class allegations in complaint is improper end-run around class certification briefing).

The sole case in NBEO's entire brief where class allegations were stricken prior to a motion for class certification, the out-of-circuit *In re Zappos.com, Inc.*, No. 2357, 2016 WL 2637810 (D. Nev. May 6, 2016), is nothing like the instant action. *Zappos* involved a case filed in early 2012, with the court striking certain class allegations years later in May 2016 after some discovery and the facts of the case had time to develop. By contrast, here the case is only two months old and no discovery has occurred or been permitted. The *Zappos* court had also previously warned the plaintiffs that it did not agree with their proposed class, a warning the plaintiffs failed to heed. *Id.* at *8. Moreover, the *Zappos* court agreed with the prevailing view that "[i]n most cases, a district court should 'afford the litigants an opportunity to present evidence as to whether a class action was maintainable,' because 'often the pleadings alone will not resolve the question of class certification and [thus] some discovery will be warranted.'" *Id.* at *7 (quoting *Doninger v. Pac. Nw. Bell, Inc.*, 564 F.2d 1304, 1313 (9th Cir. 1977)).

[12] To the extent the Court is inclined to resolve the suitability of this case for class treatment now, Plaintiffs request leave to file a supplemental brief addressing each of the elements of Rule 23 as they relate to Plaintiffs' allegations and the evidence Plaintiffs have gathered including subsequent to the filing of the Complaint.

[13] NBEO cites no authority for its additional rationales for striking Plaintiffs' allegations, including that the allegations may instill fear in or unduly influence the fact finder, or may place an undue burden on NBEO to respond. *See* Doc. 11-1 at 31-32. NBEO's citation to *Xerox Corp. v. ImaTek, Inc.*, 220 F.R.D. 241 (D. Md. 2003) is misplaced, as there the stricken material was deemed not to "relate in any way to either parties' claims." *Id.* at 243. By contrast, as detailed herein, the allegations NBEO seeks to strike relate directly to Plaintiffs' claims.

to be stricken it must have "no possible relation to the controversy." *United States ex rel. Ackley v. IBM*, 110 F. Supp. 2d 395, 405 (D. Md. 2000).

NBEO fails to meets it burden of showing that any of the allegations at issue are immaterial, prejudicial, and have no possible relation to the action. Paragraphs 21-23 of Plaintiffs' Complaint allege recent prior data breaches in the field of higher education which are facts supporting Plaintiffs' contention that NBEO knew or should have known of the risk of a data breach and that the resulting harm was foreseeable. *See* Compl., ¶ 53. At paragraphs 26, 30 and 31, Plaintiffs allege the harm that results from having one's identity stolen, the time that must be spent to resolve problems arising from identity theft, and the uncertainty victims face in determining when harm will occur. These allegations go directly to Plaintiffs' allegations of the harm they are continuing to suffer and the need for mitigating measures like credit monitoring. Thus, each of these allegations is highly germane to Plaintiffs' claims. Accordingly, the Court should deny NBEO's motion to strike any allegations from the Complaint.

CONCLUSION

For the foregoing reasons, NBEO's motion to dismiss Plaintiffs' claims and/or to strike their allegations must be denied.

Dated: November 10, 2016

Respectfully submitted,

By: s/ Norman E. Siegel

Norman E. Siegel (*pro hac vice*)
Barrett J. Vahle (*pro hac vice*)
J. Austin Moore (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City MO 64112
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com
Tel: (816) 714-7100
Fax: (816) 714-7101

Hassan Zavareei No. 18489
TYCKO & ZAVAREEI LLP
1828 L. Street, NW, Suite 1000
Washington, DC 20036
hzavareei@tzlegal.com
Tel: (202) 973-0910
Fax: (202) 973-0950

Counsel for Plaintiffs and the Class

CERTIFICATE OF SERVICE

I hereby certify that on November 10, 2016, I filed the foregoing document via the Court's ECF system, which will cause a true and correct copy of the same to be served electronically on all ECF-registered counsel of record.

/s/ Norman E. Siegel
Counsel for Plaintiff