IN THE UNITED STATES DISTRICT COURT

OF THE DISTRICT OF MARYLAND

BALTIMORE DIVISION

PAMELA CHAMBLISS and SCOTT ADAMSON, individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	
v.	)	Case No. 1:15-cv-02288-RDB
CAREFIRST, INC., a Maryland corporation, CAREFIRST OF MARYLAND, INC., a Maryland Corporation, and DOES 1-10,	)	
Defendants.	)	

PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS THE COMPLAINT

Price O. Gielen NEUBERGER, QUINN, GIELEN, RUBIN & GIBBER, P.A. One South Street, 27th Floor Baltimore, Maryland 21202 Telephone: (410) 332-8584 Facsimile: (410) 332-8561 Email: pog@nqgrg.com *Attorney for Plaintiff*	William B. Federman FEDERMAN & SHERWOOD 10205 N. Pennsylvania Avenue Oklahoma City, OK 73120 Telephone: (405) 235-1560 Facsimile: (405) 239-2112 Email: wbf@federmanlaw.com *Attorney for Plaintiff* *(Pro Hac Vice to be Sought)*

November 5, 2015

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

COME NOW Plaintiffs Pamela Chambliss and Scott Adamson ("Plaintiffs") and submit the following response in opposition to *Defendants' Motion to Dismiss the Complaint*, 09/24/2015, Dkt. No. 11 ("the Motion"). For the reasons set forth herein below, Plaintiffs respectfully request that the Motion be denied. Alternatively, if the Court finds any of Plaintiffs' claims are subject to dismissal, Plaintiffs respectfully request leave to amend as further discussed herein.

I. INTRODUCTION

Plaintiffs are or were insureds of Defendants CareFirst, Inc. and CareFirst of Maryland, Inc., ("Defendants"), whose personal information was compromised as a result of the data breached first disclosed by Defendant in May 2015. Defendants, in their Motion, assert that data theft is a "common occurrence" as if that somehow excuses them from culpability for failing to take the reasonable, necessary steps to protect the plethora of sensitive, highly confidential personal and medical information in their possession and the harms that their insureds suffer as a result of that failure. *Brief* at 1.[1] Defendants cannot get off so easily. In fact, the commonness of such breaches actually makes each subsequent breach all the more egregious. Just as the landlord in a high-crime area can be held liable when he fails to install a secure lock on a tenant's door and a criminal breaks into a tenant's apartment and harms her as a result, *see e.g. Lay v. Dworman*, 732 P.2d 455 (Okla. 1987), so, too, can a health insurer, who knows of the risk of cyberattack, be liable when it fails to secure its insureds' confidential personal information.

It has long been known that the healthcare sector was vulnerable to attack. Indeed, the Washington Post published an article on this very issue in 2012. *See e.g.* https://www.washingtonpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html. Later, in April

[1] "*Brief*" refers to *Memorandum in Support of Defendants' Motion to Dismiss the Complaint*, filed 09/24/2015, Dkt. No. 11-2.

of 2014, the Federal Bureau of Investigation ("FBI") warned healthcare providers that their cybersecurity systems were lax compared to other sectors and were vulnerable to attack. *See* http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423#XqCYkfq5JyLARlUK.97. This, combined with the treasure trove of information that healthcare providers are privy to, makes them a prime target for cyberattack. *See* http://dcinno.streetwise.co/2015/05/25/carefirst-hack-data-breach-facts-analysis-threats-to-customers/. Defendants knew all this but still failed to secure the sensitive, confidential personal information in its possession by taking reasonable measures such as encrypting the data to prevent thieves from using the data stored on their systems. *See* http://dcinno.streetwise.co/2015/05/20/dc-healthcare-insurer-carefirst-hacked-cyber-fireeye-hired/ ("Not only should the database have been encrypted, but access to the database should have been protected by 2-factor authentication").

Defendants assert that Plaintiffs were not actually harmed by Defendants failure to secure Plaintiffs personal information and, therefore, Plaintiffs do not have standing to bring this case. *Brief* at pp. 5-15. However, as further discussed herein, Plaintiffs have been harmed and do have standing to bring this action. Defendants also, alternatively, argue that, even if Plaintiffs did suffer harm as a result of the breach, they are not entitled to relief. *Brief* at pp. 15-23. For the reason set forth below, both arguments fail.

II. BACKGROUND

Defendants are a managed healthcare conglomerate offering health insurance products in Maryland, Virginia and the District of Columbia. *Complaint* at ¶ 10.[2] Healthcare intuitions, like Defendants, are, necessarily, gather and are privy to sensitive confidential personal and medical information. *Id.* at ¶ 11. This, combined with the fact that the industry is known to be lax in

[2] "*Complaint*" refers to the *Class action Complaint*, filed 08/06/2015, Dkt. No. 1.

implementing data security measures, makes them an especially rich and tempting target for cyberattacks. *Id.* at ¶ 15. *See* http://dcinno.streetwise.co/2015/05/25/carefirst-hack-data-breach-facts-analysis-threats-to-customers/.

In 2014, Defendants experienced a cyberattack. The attack allowed the hackers to obtain Plaintiffs' and other class members' confidential personal information – including their name, subscriber ID, e-mail address, date of birth and the user name chosen by the insured to access Defendants' website – of over a million of their insureds. *Id.* at ¶¶ 14-15. Although the breach occurred in 2014, Defendants, supposedly, did not discover the breach for a year and did not acknowledge it until May 20, 2015, and then only after the New York Times published an article announcing that Defendants had been breached. *Id.* at ¶¶ 12-14. *See* http://www.nytimes.com/2015/05/21/business/carefirst-discloses-data-breach-up-to-1-1-million-customers-affected.html?_r=0. In fact, Defendants were well aware of the risk of a security breach and the fact that a breach had taken place in 2014 but, nevertheless, failed to take the reasonable and necessary steps to protect Plaintiffs' sensitive, confidential, personal information in their possession and then failed to even acknowledge and advise insureds of the breach for a year. *Complaint* at ¶¶ 20, 43-45, 72.

While Defendants claim that the attackers did not obtain the insureds' passwords and, therefore, could not have accessed the insureds' medical information, claims information, social security number, credit card or other financial information, the experience of some plaintiffs suggests that the attackers did, in fact, obtain this information. However, even if this information was not stolen, Plaintiffs are still at risk because the hackers can use the stolen information to

masquerade as CareFirst and phish[3] for additional information from insureds. *See* http://dcinno.streetwise.co/2015/05/25/carefirst-hack-data-breach-facts-analysis-threats-to-customers/. As explained by one security expert:

> While CareFirst stated that social security numbers and credit cards were not held in the database, access to names, birth dates, and email addresses can lay the groundwork for future intelligence gathering and cyber intrusions. *Without strong encryption and access management, expect medical fraud and identity theft to run unchecked*…

http://dcinno.streetwise.co/2015/05/20/dc-healthcare-insurer-carefirst-hacked-cyber-fireeye-hired/ (emphasis added). Indeed, Plaintiffs have experienced phishing since the breach.

Plaintiffs have already been harmed by Defendants failures and the continued threat of identity theft and other harms as result of this breach is very real. *Complaint* at ¶ 21. Defendants recognize this and have offered a very insufficient two years of free credit monitoring to affected persons. *See* http://carefirstanswers.com/. Indeed, cyber security experts recommend that persons affected by a known security breach act promptly to try to protect their information from use/misuse by criminal by, for example, placing a credit alert on their file and signing up for credit monitoring without waiting for action by Defendants. *See e.g.* http://www.tomsguide.com/us/carefirst-data-breach,news-20960.html. Plaintiffs could not do this for a year because Defendants, who were the sole party with knowledge of the data breach, failed to timely advise Plaintiffs of the hack. Plaintiffs have expended, and will continue to expend, time and incurred expense in an effort to thwart criminals' use or misuse of their stolen data. *See e.g. Complaint* at ¶ 73.

[3] To "phish" means to try to obtain financial or other confidential information, typically by sending an e-mail that looks as if it is from a legitimate source but actually links to a face website that replicates the real one. *See http://dictionary.reference.com/browse/phishing*.

III. LEGAL STANDARD

"A Rule 12(b)(6) motion constitutes an assertion by a defendant that, even if the facts alleged by a plaintiff are true, the complaint fails as a matter of law 'to state a claim upon which relief can be granted'." *Jenkins v. Kurtinitis*, 2015 WL 1285355 at *5 (D. Md. Mar. 20, 2015). In considering a Rule 12(b)(6) motion, the Court must proceed "on the assumption that all the allegations in the complaint are true (even if doubtful in fact)." *SD3, LLC v. Black & Decker (U.S.) Inc.*, 801 F.3d 412, 428 (4th Cir. 2015) (quoting *Twombly*, 550 U.S. at 555, 127 S.Ct. 1955). To assess whether a complaint states a claim for relief, the Court must consider the pleading requirements of FED. R. CIV. P. 8(a)(2), which provides that a complaint must contain a "short and plain statement of the claim showing that the pleader is entitled to relief." *Jenkins*, 2015 WL 1285355 at *5. The purpose of the rule is to provide the defendant with "fair notice" of the claim and the "grounds" for entitlement to relief; "detailed factual allegations" are not necessary. *Id.* (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–56 (2007)).

Rather, to satisfy the minimal requirements of Rule 8(a) (2), the complaint need only set forth "enough factual matter (taken as true) to suggest" a cognizable cause of action. *Twombly*, 550 U.S. at 556. So long as the complaint contains contain facts sufficient to "state a claim to relief that is plausible on its face," it is sufficient. *Id.* at 570. *See also Iqbal*, 556 U.S. at 684. "Rule 12(b)(6) does not countenance dismissals based on a judge's disbelief of a complaint's factual allegations." *SD3*, 801 F.3d at 428 (quoting *Colon Health Ctrs. of Am., LLC v. Hazel*, 733 F.3d 535, 545 (4th Cir. 2013)).

IV. ARGUMENT AND AUTHORITIES

A. PLAINTIFFS HAVE ARTICLE III STANDING TO SUE.

Defendants argue that Plaintiffs do not have Article III standing and, therefore, cannot bring this action on behalf of themselves and a class of similarly situated persons. *Brief* at pp. 5-15. The question of standing is "whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues." *Warth v. Seldin*, 422 U.S. 490, 498, 95 S.Ct. 2197, 2205 (1975). Since the federal courts are constitutionally limited to hearing "cases" and "controversies," U.S. CONST., Art. III, § 2, the doctrine of standing has developed to "identify those disputes which are appropriately resolved through the judicial process." *Whitmore v. Arkansas*, 495 U.S. 149, 155, 110 S.Ct. 1717, 1722 (1990). One must not confuse "weakness on the merits" with "absence of Article III standing." *Arizona State Legislature v. Arizona Independent Redistricting Comm'n*, __ U.S. __, 135 S.Ct. 2652, 2663 (2015) (quoting *Davis v. United States*, __ U.S. __, 131 S.Ct. 2419, 2434, n. 10, (2011); *see Warth v. Seldin*, 422 U.S. 490, 500, 95 S.Ct. 2197 (1975) (standing "often turns on the nature and source of the claim asserted," but it "in no way depends on the merits" of the claim)). "To establish Article III standing, an injury must be concrete, particularized, and actual ***or*** imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Internat'l. USA*, __ U.S. __, 133 S.Ct. 1138, 1147 (2013) (citing *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149, 130 S.Ct. 2743, 2752, (2010)) (emphasis added). *See also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560, 112 S.Ct. 2130, 2136 (1992). The causal connection requirement is met if the injury sought to be redressed is "fairly can be traced to the challenged action of the defendant." *Simon v. Eastern Kentucky Welfare Rights Org.*, 426 U.S. 26, 42, 96 S.Ct. 1917, 1926 (1976). As set forth herein, Plaintiffs *do* have standing to bring this action.

1. General Principles of Injury for Article III Standing

Defendants' standing argument is predicated on a strained interpretation of *Clapper*. In *Clapper*, the ACLU sought a declaratory judgment to halt new provisions of a federal statute that allowed the National Security Agency to monitor certain communications. Notably, the ACLU filed suit before the challenged surveillance began. 133 S. Ct. 1138. Not surprisingly, 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. at 1148.

Clapper does not represent a sea change in standing jurisprudence or immunize companies from liability for negligence. Rather, *Clapper* merely confirms 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 n.5 (quoting *Monsanto*, 561 U.S. at 153).

This case is not like *Clapper*. First, it does not implicate national security or separation of power concerns, which require "especially rigorous" standing analyses. *Id.* at 1147. Second, this case does not involve the "highly attenuated chain of possibilities" presented in *Clapper*. *Id.* at 1148. Plaintiffs face real, concrete and "certainly impending" continued threats stemming from the sale of their personal information and have incurred costs to avoid them. In fact, the Supreme Court recently reaffirmed that harm having already occurred is "good evidence" of future harm. *See Susan B. Anthony List v. Driehaus*, __ U.S. __, 134 S. Ct. 2334, 2345 (2014) (distinguishing *Clapper* on this basis).

This case is more akin to *Monsanto*, where the Supreme Court held that a bee's anticipated pollination patterns create a sufficiently imminent risk of injury to farmers who feared gene flow

from genetically modified plants planted in nearby fields. 561 U.S. 139. Faced with similar facts, lower courts also have consistently recognized Article III standing, even where, unlike here, no actual misuse of compromised information has occurred. *See, e.g., Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) ("injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142 (9th Cir. 2010) (plaintiffs "whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing under Article III"). Likewise here, Plaintiffs who stand to suffer future injuries have standing to sue.

2. Analysis of Standing in Data Breach Cases

Although there are not published decisions from either this District or the Fourth Circuit, several other Circuits and District Courts have addressed the issue of standing in data breach cases. The Eleventh Circuit, for example, has found that an injury in fact occurs when "Plaintiffs allege that they have become victims of identity theft and have suffered monetary damages as a result." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 (11th Cir. 2012). In *AvMed*, criminals opened financial accounts in the plaintiffs' names and then made fraudulent charges or overdrew the accounts. *Id.* The court held that allegations of monetary injury were sufficient to confer standing. *Id.* In *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015), the Seventh Circuit reversed the district court's dismissal of a data breach class action for lack of standing. The Seventh Circuit held that the probability of future harm is imminent in the face of stolen customer data because "[w]hy else would hackers break into a store's database and steal consumers' private

information?" *Id.* at 693.[4] The Seventh Circuit further held that mitigation expenses "easily qualif[y] as a concrete injury" sufficient to confer standing under *Clapper*. *Id.* at 694. Moreover, "[i]t is telling… that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers… It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded." *Id.* Defendants, too, are offering credit monitoring, https://krebsonsecurity.com/2015/05/carefirst-blue-cross-breach-hits-1-1m/, showing that they, too, recognize that the risk of use/misuse of the stolen data is not remote or speculative but, rather, real and imminent.

Other courts have held that similar allegations conferred standing in data breach cases. For example, in *In re Target Corp. Data Sec. Breach Litig.*,[5] which dealt with facts and claims almost identical to this case, the court swiftly disposed of the argument that consumers did not allege sufficient injury:

> Plaintiffs have alleged injury. Indeed, [the Complaint recites] many of the individual named Plaintiffs' injuries, including unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees. Target ignores much of what is pled, instead contending that because some Plaintiffs do not allege that their expenses were unreimbursed or say whether they or their bank closed their accounts, Plaintiffs have insufficiently alleged injury. These arguments gloss over the actual allegations made and set a too-high standard for Plaintiffs to meet at the motion-to-dismiss stage. Plaintiffs' allegations plausibly allege that they suffered injuries that are "fairly traceable" to Target's conduct.

[4] In contrast, the personal information at issue in *In re Science Applications Internat'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F.Supp.3d 14 (D. D.C. 2014), which Defendants rely upon extensively in the *Brief*, was taken when a thief broke a window on an employee's car and stole several items, including backup tapes. There, the personal information was not the target of the robbery so it was reasonable for the court to question the likelihood of identity theft occurring as a result of the theft of the backup tapes. *Id.* at 25. In *Neiman Marcus*, *Target*, etc., the thieves specifically targeted personal information of a type that is known to be readily used to commit identify theft (social security number, date of birth, etc.) so the risk of the stolen information being used for nefarious purposes is far more immediate.

[5] 66 F.Supp.3d 1154 (D. Minn. 2014).

Target, 66 F.Supp.3d at 1159. Other courts analyzing data breach cases post-*Clapper* agree. For example, the *Sony* court found that "Plaintiffs' allegations that their Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion [were] sufficient to establish Article III standing at this stage in the proceedings." *In re Sony Gaming Networks and Customer Data Breach Security Litig.*, 996 F. Supp. 2d 942, 962 (S.D. Calif. 2014). Likewise, in *Adobe*, 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. *In re Adobe Systems, Inc. Privacy Litig.*, 2014 WL 4379916 at *2 (N.D. Calif. Sept. 4, 2014). The court found that "the threatened harm alleged here is sufficiently concrete and imminent to satisfy *Clapper*" because "the risk that Plaintiffs' personal data will be misused by the hackers… is immediate and very real." *Id.* at *8. There, as here, speculation was not required as "stolen data had already surfaced on the internet." *Id.* 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 Moyer v. Michaels Stores, Inc.*, 2014 WL 3511500 at *6 (N.D. Ill. July 14, 2014) ("elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent").

3. Plaintiffs Have Suffered an Injury-in-Fact

Some plaintiffs have had their personal information used or misused as a result of the data breach. Others have spent time and/or incurred expenses to prevent or, at least, reduce the potential damage from the use or misuse of their data. These injuries are real, immediate and non-speculative. *See F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 625 (D.N.J. 2014) (finding data breach has potential to cause "substantial injury" to consumers). Defendants argue that the time and expense incurred by Plaintiffs to avoid or minimize the damage from the use or

misuse of their personal information does not grant standing. *Clapper*, however, recognized that in cases where there is a substantial risk harm will occur, plaintiffs may be prompted "to reasonably incur costs to mitigate or avoid that harm." *Clapper*, at 1150, n.5 (citing Monsanto, 561 U.S. at 153-54). *See also Adobe*, at *9 ("costs incurred in an effort to mitigate the risk of future harm constitute injury-in-fact"); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164 (1st Cir. 2011) (where plaintiffs face imminent harm,"[t]he question then becomes whether plaintiffs' mitigation steps were reasonable."). Plaintiffs acted reasonably in trying to remedy, limit, and prevent the vast array of injuries described above. Additionally, plaintiffs would not have continued doing business with Defendants had they known of the breach and/or that Defendants were not securely storing their confidential information. Those "would not have shopped" or "would not have purchased" damages are sufficient to allege actual damages. *See*, generally, *Target*, 66 F.Supp.3d at 1166. Moreover, contrary to Defendants' assertion, the mere passage of time, (one year in this instance), does not mean that Plaintiffs' injuries are not fairly traceable to the breach. *See e.g. Esklin v. The Coco-Cola Company*, __ F.Supp.3d __, 2015 WL 5729241 at *7 (E.D. Penn. Sept. 30, 2015) (holding that injuries were fairly traceable even though seven years had passed).

Finally, standing may be grounded upon the invasion of statutory or common law rights. The violation-of-rights doctrine has been applied in recent privacy *litigation. See In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *17 (N.D. Cal. Sept. 26, 2013) ("[a]ll Plaintiffs need allege is an invasion of statutory. . . rights to survive a motion to dismiss on standing grounds"). Plaintiffs have a statutory and common law right of privacy. *See e.g.* MASS. ST. 214 §1B, MASS. ST. 93A §9(3). That right was violated by Defendants' failure to take reasonable precautions against a security breach. Plaintiffs have standing for this reason as well.

B. PLAINTIFFS ADEQUATELY PLED EACH OF THEIR CLAIMS AGAINST DEFENDANTS.

1. Plaintiffs Have Adequately Pled Claims for Negligence and Have Alleged Actual Damages.

Defendants assert that "Count I of the Complaint (Plaintiffs' claim for negligence) must be dismissed for failure to plead damages." *Brief* at 15. However, in the Complaint now at issue, damage-related allegations include, *inter alia*:

> As a result of CareFirst's deficient practices, Plaintiffs and the class members have been damaged, and have lost or are subject to losing money and property as a result of CareFirst's substandard security practices.
>
> As a result of CareFirst's conduct, Maryland Plaintiff and the Maryland Class members will incur economic damages related to the expenses for credit monitoring and the loss associated with paying for health services they believed were purchased through secure transactions. Maryland Plaintiff and the Maryland Class members would not have purchased the health insurance and other services had they known that their PI would be compromised.

Complaint at ¶¶ 21, 73.

Moreover, this action is at the very earliest stages of litigation. To withstand a motion to dismiss, Plaintiffs need only provide sufficient factual allegations from which the Court can make the "reasonable inference" that Defendants are liable for the misconduct alleged. *Iqbal,* 556 U.S. at 678. Defendants' arguments about the sufficiency of the damage allegations of the *Complaint* are premature. Plaintiffs have pled a "short and plain statement" of their claims as required by Fed.R.Civ.P. 8(a)(2). Discovery will be required to flesh out the exact categories of actual damages such as customers' remedial costs related to improper use of personal or medical information. In addition, many, if not most plaintiffs, will be entitled to recover what other courts in the data breach arena have called "would not have shopped" damages. That is, had Plaintiffs known their personal and medical information would not be secure, they would have obtained their medical insurance elsewhere. *See e.g. Target*, 66 F.Supp.3d at 1166.

Moreover, Plaintiffs have alleged that Defendants should have known about the data breach immediately. Defendants announced in May 2015 that they previously suffered a data breach in June 2014 – nearly a *year* after the fact. Defendants' announcement, on May 20, 2015, was probably not coincidentally the same day the New York Times published a story about the same data breach. With regard to healthcare data breaches, such as this one, one expert opined to the New York Times: "It's such an attractive target and it's a soft target and one not traditionally well protected."[6] Notwithstanding the likely knowledge it was seen as a soft target, Defendants had not implemented sufficient protective measures to ensure the privacy of its customers' personal and medical information. *See Complaint* at ¶¶ 13-21. Assuming the truth of these allegations, which is the standard by which this Court must be guided, nearly every putative class member will be able to claim the aforementioned actual damages including "would not have shopped" damages from Defendants. *See, e.g. Target*, 66 F.Supp.3d at 1166. As such, the Motion must be denied with respect to Count I.

2. Plaintiffs Negligence Claims Are Not Barred by the "Economic Loss Rule."

Courts that have considered the "economic loss rule" vis-a-vis negligence claims under Maryland law have held the rule not to apply when some extra-contractual duty has been alleged. "A contractual obligation, by itself, does not create a tort duty. Instead, the duty giving rise to a tort action must have some independent basis." *Mesmer v. Maryland Auto Insurance Fund*, 353 Md. 241, 253, 725 A.2d 1053 (1999). "The [economic loss] rule's purpose therefore is not implicated where close inspection of the plaintiff's case reveals a genuine foundation for a tort claim. In such situations, there is no risk that a plaintiff will be pursuing a tort remedy when in

[6] See, http://www.nytimes.com/2015/05/21/business/carefirst-discloses-data-breach-up-to-1-1-million-customers-affected.html?_r=0

fact he should be confined to a contract remedy. Thus, if, when the surface is scratched, it appears that the defendant has breached a duty imposed by law, not by contract, the economic loss rule should not apply." *City of Richmond v. Madison Management Group, Inc*., 918 F.2d 438, 446 (4th Cir. 1990).[7]

In *City of Richmond*, the Fourth Circuit, in analyzing the economic loss rule in the analogous circumstance where both a tort claim (fraud) and a contract claim (breach of contract) were made, stated as follows:

> *Here, the City does not allege mere failure to keep a promise. Instead, it alleges that [Defendant] knew, at the time it promised to supply conforming pipe, that it would not supply conforming pipe.* Thus, contrary to the Pipe Defendants' assertion, it is not the case [as Defendants allege] that "[t]he City's allegations of fraud constitute nothing more than a thinly-veiled recasting of its claim for breach of contract as a tort." The case at bar does not involve any such attempt to dress up a contract claim in a fraud suit of clothes.

City of Richmond, 918 F.2d at 447 (Internal citations omitted) (emphasis added.)

Similar to the facts in *City of Richmond*, here, Defendants are alleged to have implicitly if not explicitly[8] promised to keep Plaintiffs' personal and medical information safe and secure. Plaintiffs further allege that Defendants knew or should have known that their data security measures would not withstand an attack by hackers. Nonetheless, Defendants failed to correct their security deficiencies, resulting in the breach. *Complaint* at ¶ 20. Succinctly, Defendants knew from the time they implicitly or explicitly promised to provide effective data security for customers' personal and medical records that they would not be able to provide such level of data security.

3. Plaintiffs Have Adequately Pled Their Implied Contract Claim.

[7] Applying nearly analogous Virginia law.

[8] CareFirst hired Mandiant Security Consulting to advise it on solving its data security issues. Clearly, CareFirst did so to assuage its customers. Compl. at ¶ 20. It is not clear, however, what if anything Mandiant actually did.

Count II of the Complaint asserts that Plaintiffs and Defendants were party to an implied contract in which Defendants, in essence, agreed to use Plaintiffs' personal and medical information only for those ordinary and usual purposes associated with employer-sponsored health insurance, along with Defendants' implied promise to safeguard the aforementioned highly vulnerable personal and medical information of Plaintiffs. *Complaint* at ¶¶ 48-53. Defendants contend that Plaintiffs failed to adequately plead the existence of such an implied contract. However, Plaintiffs have alleged:

> By entering into agreements with Plaintiffs and Class members, either directly or with Class members as third party beneficiaries under employer-sponsored health insurance, CareFirst imposed upon itself an obligation to use reasonable and industry-standard security practices and procedures to protect Plaintiffs' and Class members' data and personal information.

Compl. at ¶ 50.

Judge Paul A. Magnuson, prior to ruling on the motion to dismiss in the *Target* case, *supra*, surveyed several similar MDL data breach cases, which had raised nearly identical implied contract claims as those of Plaintiffs. Judge Magnuson found, in reviewing the decisions of other MDL data breach courts, that the implied contract claims raised in such prior cases (which were substantively similar to those alleged here) were indeed pled sufficiently under the standards of Rule 8. *Target*, 66 F.Supp.3d at 1176-1177. Judge Magnuson, citing *In re Hannaford Bros. Customer Data Securities Breach Litigation.*, 613 F.Supp.2d 108, 118 (D. Me. 2009),[9] found that whether an implied contract exists is a question of fact and that "a jury could reasonably find that a customer's use of a credit or debit card to pay at a retailer *may include the implied contract term that the retailer will take reasonable measures to protect the [personal] information on those*

[9] Affirmed by the First Circuit in *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 158–59 (1st Cir. 2011).

cards." *Target*, 66 F.Supp.3d at 1177 (Internal quotations and citations omitted; emphasis supplied.)

Thus, the courts in *Target*, *In re Hannaford Brothers*, and *In re Michaels Stores Pin Pad Litigation*,[10] all denied motions to dismiss the implied contract claims. That is, it is a question of fact for the jury to determine whether an implied contract exists requiring any given business to protect the personal information of its customers. This Honorable Court should follow these authorities in the instant case for the reasons set forth above and for the additional reason that the data being protected by Defendants was and is not just personal identifying and financial information as was at issue in the aforementioned credit card data breaches. The data in the instant case importantly also includes highly personal medical information (which is typically a person's most private and personal information). Once can hardly imagine a more compelling case in which a jury would find the existence of an implied contract than one involving the potential or actual loss of control over customers' personal medical information.

4. Plaintiffs' Request for Declaratory Relief is Appropriate

Plaintiffs concur with Defendants to the extent Defendants urge that a declaratory judgment is a form of remedy and not technically a basis or foundation for a cause of action. *Brief* at p. 21. However, by agreeing with this basic premise, Plaintiffs are not conceding nor agreeing that they are in any manner not entitled to declaratory relief as a remedy.

[10] *In re Michaels Stores Pin Pad Litigation*, 830 F.Supp.2d 518, 528 (N.D. Ill. 2011).

5. Plaintiffs' Claims Under the Maryland Personal Information Protection Act Are Adequately Asserted and Should Not Be Dismissed.

Defendants make the attenuated argument that they are somehow exempt from the ambit of the Maryland Personal Information Protection Act ("MPIPA") because of a pre-MPIPA exemption contained in the overarching Maryland Consumer Protection Act ("MCPA") (which law was never made explicitly applicable to the MPIPA). Initially, a plain language reading of the MCPA exemption, even if it were somehow applicable, demonstrates the exemption has nothing whatever to do with Defendants. Under the MCPA, it states that the MCPA does not apply to:

> 1) The professional services of a certified public accountant, architect, clergyman, professional engineer, lawyer, veterinarian, insurance company authorized to do business in the State, insurance producer licensed by the State, Christian Science practitioner, land surveyor, property line surveyor, chiropractor, optometrist, physical therapist, podiatrist, real estate broker, associate real estate broker, or real estate salesperson, or medical or dental practitioner;

Md. Code Ann., Com. Law § 13-104 (1).

This exemption is clearly aimed at certain professional individuals and entities that are licensed and governed by special professional codes such as, for instance, lawyers whose professional conduct is governed by the licensing state's rules of professional conduct for attorneys. In the insurance area, this exemption seems plainly aimed at Maryland's licensed insurance producer agencies (i.e., insurance brokers) and Maryland's licensed insurance producers (i.e., insurance salespeople), not multi-state, regional underwriters of health insurance like Defendants.

The only known reported case on point is *Scull v. Groover, Christie & Merritt, P.C.*, 76 A.3d 1186, 435 Md. 112 (2013). In *Scull*, the plaintiff brought an action against his doctors for violation of the Maryland Health Maintenance Organization Act (the "HMO Act"), which law prohibited "balance billing" or charging fees for medical services above and beyond those allowed

by the given HMO's physician fee schedule. The doctors defended, in part, by claiming they were exempt from liability under the HMO Act by virtue of the MCPA exemption set forth in the above-cited Section 13-104 (1). However, the Maryland Court of Appeals[11] held that the Section 13-104 (1) exemption did not apply because the exemption "applie[d] only to the actual professional services of a physician . . . [not to] the commercial aspects of a medical practice, such as compliance with laws concerning who may be billed and how." *Scull*, 76 A.3d at 1197. The *Scull* Court noted as follows:

> There is no definition of "professional services" contained in the Consumer Protection Act. Nor is there any legislative history available pertaining to the 1974 enactment of what is now CL § 13–104(1). However, there is legislative history pertaining to the 2003 enactment of the related exemption in CL § 13–408 concerning the "professional services" of health care providers. Proponents of the exclusion explained the intended scope of the exclusion for "professional services" in presentations to the Consumer Protection Division and the Legislature:
>
> [T]he term "professional services" means the quality of care rendered by a health care provider in the marketplace, but it does not apply to the commercial or entrepreneurial services, such as billing, reimbursement, or advertising and marketing.

Scull, 76 A.3d at 1194.

Plainly, this lawsuit is not about the provision of professional insurance services by a professional insurance provider licensed by the Maryland Insurance Administration. Hence, under *Scull*, the Section 13-104 (1) exemption is unavailing. Additionally, CareFirst makes the assertive leap that the Section 13-104 (1) exemption of the MCPA *ipso facto* applies to claims brought under the MPIPA yet cites to nothing substantive to support that assertion. The MCPA was initially enacted by the Maryland General Assembly in 1957, with the exemptions being added in 1974. In

[11] The *Scull* court did not address the issue of whether the MCPA exemption should even apply to the asserted HMO Act claim and instead determined that the express language of the MCPA exemption made such exemption inapplicable in *Scull*. *Id.*

contrast, the MPIPA was first enacted by the General Assembly in 2008. In pertinent part, the MPIPA states its purpose as follows:

> To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.

Md. Code Ann., Com. Law § 14-3503 (a).[12]

Logically, it makes no sense to exempt Defendants from the MPIPA when Defendants would, by definition, be handling massive amounts of "personal information" of Maryland residents and, thus, Defendants would seem to be exactly the type of business the Maryland General Assembly was aiming at when first enacting the MPIPA in 2008. Under the standard rules of statutory construction, to the extent that there is a conflict between the two provisions, the later enacted provision—i.e. the MPIPA—prevails. *State v. Ghajari*, 346 Md. 101, 115, 695 A.2d 143 (1997). Moreover, as a general rule, when a specific enactment and general enactment appear to cover the same subject but the two appear to conflict, the more specific enactment (again, the text of the MPIPA) prevails. *Smack v. Department of Health & Mental Hygiene*, 378 Md. 298, 306, 835 A.2d 1175 (2003). Here, Defendants are endeavoring to "fit a square peg into a round hole" by urging that an insurance provider's exemption added in 1974 to a general law (i.e., the MCPA) somehow exempts them from compliance with the more specific MPIPA when the later enacted MPIPA contains no such exemption. Defendants argument on this point are patently baseless. Succinctly, neither the text of the MPIPA, the text of the MCPA exemption itself, *supra*, nor basic rules of statutory construction assist Defendants in claiming that the MCPA exemption should apply to them.

[12] MPIPA also requires timely notification of any data breach. See Md. Code Ann., Com. Law § 14-3504 (requiring companies to provide notice "as soon as reasonably practicable.").

Defendants second point concerning the MPIPA is that Plaintiffs have not sufficiently alleged damages for MPIPA purposes. Despite CareFirst's continual assertions concerning damages, Plaintiffs have clearly alleged substantial and meaningful damages flowing from the data breach and Defendants' concomitant unreasonable delay in notifying the Maryland Plaintiff and Maryland Class members. In this regard, Plaintiffs allege that:

> CareFirst negligently and recklessly failed to provide reasonable and adequate security measures. CareFirst also unreasonably delayed informing the Maryland Plaintiff and Maryland Class members about the security breach of Maryland plaintiff's and Maryland Class members' PI (and potentially confidential health information) after CareFirst knew the data breach had occurred.
>
> As a result of CareFirst's conduct, Maryland Plaintiff and the Maryland Class members will incur economic damages related to the expenses for credit monitoring and the loss associated with paying for health services they believed were purchased through secure transactions. Maryland Plaintiff and the Maryland Class members would not have purchased the health insurance and other services had they known that their PI would be compromised.

Complaint at ¶¶ 72, 73.

Moreover, case law holds that the MCPA (and, thus, the MPIPA) "is to be construed liberally to promote the protection of consumers." *Scull*, 76 A.3d at 1193 (Internal citations omitted). Consistent with such a "liberal construction," courts in other data breach cases (as stated in Part II (A) of this Memorandum, *supra*) have held that an allegation of "would not have shopped" or "would not have purchased" is sufficient to allege actual damages. *See*, generally, *Target*, 66 F.Supp.3d at 1166. That is, the consumer was damaged because he or she made a purchasing decision which likely would have not occurred had the consumer known the true facts and circumstances concerning Defendants lack of sufficient data security.[13] Plaintiffs respectfully

[13] In the case of CareFirst, as stated, its lack of sufficient data security resulted in the June 2014 data breach which breach was not even disclosed by CareFirst to its customers until May 2015 and then only under the "pressure" of an unflattering New York Times article.

urge this Court to hold that their Complaint's damage allegations likewise withstand Defendants' Rule 12(b)(6) motion to dismiss.

C. Alternatively, Plaintiffs should be permitted to amend.

If the Court finds that any of Plaintiffs claims are insufficiently pled, Plaintiffs request leave to amend. *See* Fed. R. Civ. P. 15(a)(2) ("The court should freely give leave [to amend] when justice so requires"). If amendment is required, Plaintiffs can add allegations, such as those discussed throughout this brief, regarding the breach, the probable consequences of it as well as the harm that Plaintiffs have suffered as a result of the breach. Additional plaintiffs, with descriptions of the harm they have suffered, may also be added. Accordingly, amendment would not be futile. Leave to amend should be granted. *Forman v. Davis*, 371 U.S. 178, 182, 83 S.Ct. 227, 299 (2003) (holding that leave to amend should be granted if the "underlying facts or circumstances" are a "proper subject of relief" so that the plaintiff is "afforded an opportunity to test his claim on the merits").

V. CONCLUSION

WHEREFORE, for the reasons set forth herein, Plaintiffs respectfully request that the Court deny *Defendants' Motion to Dismiss the Complaint*, 09/24/2015, Dkt. No. 11. Alternatively, if the Court finds that any of the claims that Plaintiffs assert is subject to dismissal, Plaintiffs request leave to amend.

Dated: November 5, 2015

Respectfully submitted,

NEUBERGER, QUINN, GIELEN, RUBIN & GIBBER, P.A.

By: /s/ Price O. Gielen
Price O. Gielen
One South Street, 27th Floor
Baltimore, Maryland 21202
Telephone: (410) 332-8584
Facsimile: (410) 332-8561
Email: pog@nqgrg.com

Attorney for Plaintiffs

-and-

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: wbf@federmanlaw.com

Attorney for Plaintiff
(Pro Hac Vice to Be Sought)

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the CM/ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on November 5, 2015.

/s/ Price O. Gielen