E-FILED
Tuesday, 23 August, 2016 03:51:51 PM
Clerk, U.S. District Court, ILCD

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS
PEORIA DIVISION

CHANDAN UNCHAGERI,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 16-1068**
	)	
CAREFIRST OF MARYLAND, INC. and GROUP HOSPITALIZATION and MEDICAL SERVICES, INC. both d/b/a CAREFIRST BLUE CROSS BLUE SHIELD,	)	
	)	
Defendants.	)	

ORDER

This matter is now before the Court on a Motion to Dismiss filed by Defendants CareFirst of Maryland, Inc. and Group Hospitalization and Medical Services, Inc. (collectively referred to as "Defendants" or "CareFirst") (ECF No. 10) pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(2), 12(b)(3), and 12(b)(6); and a Motion to Amend Putative Class Action Complaint filed by Plaintiff Chandan Unchageri ("Plaintiff") (ECF No. 15) pursuant to Federal Rule of Civil Procedure 15(a). For the reasons set forth below, Defendants' Motion to Dismiss (ECF No. 10) is GRANTED and Plaintiff's Motion to Amend (ECF No. 15) is DENIED. This matter is now TERMINATED.

BACKGROUND

The Defendants in this case are one of the largest managed health care insurers in the Mid-Atlantic, serving nearly 3.4 million members in Maryland, the District of Columbia, and portions of Northern Virginia. (ECF No. 1 at 1). Plaintiff alleges Defendants' members include Mid-Atlantic companies that provide CareFirst health care plans to their employees all across the United

States. *Id.* at 1-2. On June 19, 2014, hackers gained access to sensitive confidential data entrusted to Defendants. *Id.* at 2. The information accessed included full names; email addresses; dates of birth; and other personal information including user names and subscriber numbers or "subscriber ids" ("Personally Identifiable Information" or "PII"). *Id.* As of the day the Complaint in this case was filed, it had been reported that the data breach compromised the data of up to 1.1 million people, including current and former CareFirst members and their employees, and individuals who do business with CareFirst online. *Id.* Plaintiff had medical insurance coverage through CareFirst BlueCross BlueShield on June 19, 2014. *Id.* at 4.

Plaintiff alleges Defendants detected the hack initially on a date on or after June 19, 2014, but prior to April 21, 2015. *Id.* at 2. Plaintiff alleges Defendants incorrectly concluded no member information was accessed and failed to take any action to notify its members that PII information might be at risk within a reasonable time prior to May 22, 2015. *Id.* On May 22, 2015, Defendants revealed they had suffered a catastrophic data breach of their information technology system ("Network"). *Id.* at 1. Plaintiff alleges Defendants suffered the catastrophic data breach because they failed to develop, maintain, and implement sufficient security measures on their computer networks, particularly given the fact that their systems harbor medical and other private data. *Id.* at 2. Plaintiff alleges Defendants failed to reasonably protect PII, and in the summer of 2015, the Federal Bureau of Investigation issued a warning that the health care industry might be targeted by hackers. *Id.* Nonetheless, Plaintiff alleges Defendants failed to take these warnings to heart and let close to a year elapse before purportedly detecting the data breach and/or detecting that the data breach compromised the data of CareFirst members and their employees. *Id.*

Plaintiff alleges the data breach at issue in this case follows in the wake of widely publicized data breaches affecting companies such as Target; Home Depot; Neiman Marcus;

Community Health Systems, Inc.; Michaels Stores; Jimmy Johns; Sony Pictures Entertainment; J.P. Mortgage Chase & Co.; P.F. Chang's; and Staples among others. *Id.* at 2-3. Notably, Plaintiff alleges similar attacks specific to health insurance databases have recently affected Anthem, Inc. (and its affiliated companies Anthem and Empire Blue Cross Blue Shield, Caremore, HealthLink, and UniCare) and Premera Blue Cross, demonstrating targeted efforts to obtain the healthcare information of millions of individuals. *Id.* at 3. Notwithstanding these earlier data security incidents, particularly those at associated Blue Cross and Blue Shield companies, Plaintiff alleges Defendants failed to take adequate steps to prevent the data breach at issue in this case from occurring. *Id.* at 4.

Plaintiff alleges that despite Defendants' claim that the single hacked database contained "only" the above-mentioned PII, Defendants maintain databases that include individual's social security numbers; medical information; claims information; financial information; and account passwords. *Id.* Plaintiff alleges that under Defendant's deficient policies, access to the hacked database provides a hacker with sufficient PII to change the user's password and gain access to consumers' accounts and other databases which include invaluable personal, medical and financial information. *Id.* Plaintiff alleges Defendants' reaction to the data breach has been anemic at best, and Defendants failed to timely notify affected consumers including Plaintiff. *Id.* Plaintiff alleges Defendant's proposed "solution," offering credit monitoring protection for a period of two years, is a woefully deficient approach. *Id.* Plaintiff alleges consumers face a lifelong battle to control the damages of their PII being stolen by hackers, including fraudulent tax returns, stolen identities, and/or medical identity fraud. *Id.* Plaintiff alleges Defendants' failure to adequately protect PII has caused, and will continue to cause, substantial customer harm and injuries to Defendants' members and employees across the United States. *Id.*

Plaintiff alleges that in its "carefully crafted" responses to purportedly "frequently asked questions," CareFirst emphasized that "the database accessed by attackers contained no member [s]ocial [s]ecurity numbers, medical claims, employment, credit card, or financial information." *Id.* at 5-6. Plaintiff alleges CareFirst also attempted to placate consumers by stating ""[t]he information accessed as part of this attack is of limited utility to others . . . The user name alone cannot be used to access member information without the associated password." *Id.* at 6. Plaintiff alleges that despite CareFirst's claims that the hacked database did not contain user passwords, it contained valuable PII and enabled access to databases that contained other valuable PII, including social security numbers, medical, credit card, and financial information. *Id.* After the data breach, CareFirst enabled online account subscribers, or anyone providing a subscriber's information to change that subscriber's password. *Id.* Plaintiff alleges this change can be, and was, accomplished using only PII accessible in the hacked database. *Id.* Thus, Plaintiff alleges that in addition to the valuable non-financial PII hackers obtained, hackers were and are able to access personal, medical and financial information as a direct and foreseeable result of CareFirst's failure to maintain the privacy and security of Plaintiff's and the putative class members' PII. *Id.*

Plaintiff alleges that contrary to CareFirst's empty assurance, non-financial PII is highly sought after information. *Id.* Plaintiff alleges that as reported by *CreditCards.com*, hackers are looking to steal non-financial information so they can continue to monetize victims' identities over a longer period of time. *Id.* at 7. Plaintiff alleges that once use of compromised non-financial PII is detected, the emotional and economic consequences to its owners are significant. *Id.* Plaintiff alleges that despite CareFirst's own promises to maintain data security, and the critical nature of maintaining the security of consumers' personal information, "upon information and belief," CareFirst did not take steps to encrypt the sensitive PII of its customers that it maintained. *Id.* at

8. Plaintiff alleges CareFirst did not disclose to anyone that it did not have adequate security systems in place to keep Plaintiff and other customers' personal and health information that CareFirst maintained on its computer systems private and secure. *Id.*

Plaintiff alleges his putative class action Complaint asserts claims on behalf of a nationwide class and subclasses which consist of individuals who had their data stolen from CareFirst's systems as follows:

> All persons in the United States whose personal, medical or financial information was compromised by the data breach that occurred on or around June 19, 2014, and disclosed by CareFirst on or around May 22, 2015, (the "National Class").
>
> All persons in Illinois whose personal, medical or financial information was compromised by the data breach that occurred on or around June 19, 2014, and disclosed by CareFirst on or around May 22, 2015, (the "Illinois Class").

Id. at 9-10. Plaintiff alleges Defendants, their CEO, and the Judges assigned to this case are excluded from the aforementioned class. *Id.* at 10.

PROCEDURAL HISTORY

On February 23, 2016, Plaintiff filed the putative class action Complaint in this case. (ECF No. 1). The Complaint alleges: (1) negligence; (2) negligence per se; (3) breach of implied contract; (4) violation of Illinois Consumer Fraud Act and Illinois Privacy Protection Act; (5) violation of Illinois Insurance Code; and (6) unjust enrichment. (ECF No. 1 at 12-18). On April 29, 2016, Defendants filed a Motion to Dismiss, which is currently before the Court, and the Response was due by May 16, 2016. (ECF No. 10). In the Motion, Defendants put the court on notice of the fact that this case is the third similar putative class action to be filed arising out of the same data breach, with the other two cases being in the United States District Court for the District of Columbia, and the United States District Court for the District of Maryland. (ECF No. 10-1 at 2). On May 4, 2016, Plaintiff filed an unopposed Motion to Extend Briefing Schedule. (ECF No.

13). On May 9, 2016, via Text Only Order, the Court granted Plaintiff's Motion and ordered Plaintiff to file his Response on or before June 10, 2016. *See* Text Only Order dated 5/9/2016. On June 6, 2016, Defendants filed a Notice of Related Decision putting the Court on notice of a decision in the companion case in the United States District Court for the District of Maryland. (ECF No. 14). On June 9, 2016, Plaintiff's counsel requested Defendants' consent to file an Amended Putative Class Action Complaint. (ECF No. 16-1 at 1). On June 10, 2016, at 10:59 a.m., Defendants' counsel replied to Plaintiff's counsel's request by stating, among other things, "[w]e cannot, at this time, consent to the filing of an amended complaint, particularly without having an opportunity to see a draft." (ECF No. 16-2 at 1). Thereafter, on June 10, 2016, at 6:13 p.m., Plaintiff filed a Motion to Amend Putative Class Action Complaint, which is currently before the Court. (ECF No. 15).

On June 23, 2016, Defendants filed a Memorandum in Opposition to Plaintiff's Motion to Amend. (ECF No. 16). On August 4, 2016, via Text Only Order, the Court stated that, "[i]n reviewing the Motion to Amend the Court notes paragraph 48 of the proposed Amended Complaint is not specific enough with respect to whether or not the alleged unauthorized charges resulted from the data breach at issue in this case. As such, Plaintiff has 14 days from the entry of this Order to file a document with the Court clarifying exactly what he is talking about." *See* Text Only Order dated 8/4/2016. On August 12, 2016, Defendants filed a Notice of Related Decision putting the Court on notice of a decision in the companion case in the United States District Court for the District of Columbia. (ECF No. 17). On August 19, 2016, Plaintiff filed a Memorandum in compliance with the Court's August 4, 2016, Text Only Order. (ECF No. 18).

DISCUSSION

"As a general matter, Federal Rule of Civil Procedure 15 ordinarily requires that leave to amend be granted at least once when there is a potentially curable problem with the complaint or other pleading. A plaintiff is entitled to amend the complaint once as a matter of right, and a court should freely give leave for a party to file an amended complaint when justice so requires. A district court may deny leave to file an amended complaint in the case of undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, and futility of amendment." *Bausch v. Stryker Corp.*, 630 F.3d 546, 562 (7th Cir. 2010)(internal citations and quotations omitted). "District courts may refuse to entertain a proposed amendment on futility grounds when the new pleading would not survive a motion to dismiss." *McCoy v. Iberdrola Renewables, Inc.*, 760 F.3d 674, 685 (7th Cir.), reh'g denied, 769 F.3d 535 (7th Cir. 2014)(internal citations omitted).

When considering whether a plaintiff has Article III standing to bring a claim, the Supreme Court has stated "the irreducible constitutional minimum of [Article III] standing contains three elements. First, the plaintiff must have suffered an injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be fairly . . . traceable to the challenged action of the defendant, and not . . . the result of the independent action of some third party not before the court. Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. The party invoking federal jurisdiction bears the burden of establishing these

elements." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)(internal citations and quotations omitted); *See also* (ECF No. 14-1 at 5).

When a lawsuit is a putative class action, any named plaintiff "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Warth v. Seldin*, 422 U.S. 490, 502 (1975). "[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974).

In his Motion to Amend, Plaintiff argues that since the filing of his original Complaint events have arisen which, while unnecessary for the purposes of pleading the original Complaint, are germane to Defendants' Motion to Dismiss. (ECF No. 15 at 1). Plaintiff's counsel alleges that in drafting Plaintiff's Response to Defendants' Motion to Dismiss and consulting with Plaintiff, Plaintiff's counsel was apprised that in approximately April 2016 Plaintiff was subjected to further anxiety and damages resulting from the misuse of the data obtained from the data breach at issue. *Id.* at 2. Specifically, Plaintiff alleges he received at least two outrageous and frightening telephone calls from persons in possession of the very data at issue in this case. *Id.* Plaintiff alleges several persons masquerading as agents of the IRS represented to him that he was in violation of unspecified tax laws and owed the IRS approximately $2,800.00. *Id.* Plaintiff alleges the persons on the phone verified themselves by providing him with his full name, address, date of birth, cellular telephone number, and e-mail address. *Id.*

Plaintiff alleges these individuals demanded immediate payment over the phone to the IRS for the tax violation or be subject to immediate arrest by the Bloomington Police. *Id.* Plaintiff alleges he was warned the IRS had frozen his credit cards, his passport had been revoked, and he

would need to pay by providing his bank account and routing number for a wire transfer. *Id.* Plaintiff alleges that after being passed on to a "supervisor" who identified herself as a "tax processer" he was threatened with immediate arrest as a result of his unwillingness to immediately comply. *Id.* Several weeks later, Plaintiff alleges he received another of these calls with substantially similar threats, but with one significant difference, the caller asked Plaintiff to look at his caller ID to see the 800 number from which the call was coming, and to Google it to confirm this number was indeed the IRS' 800 number. *Id.* Plaintiff argues that while the aforementioned allegations are not necessary for the elements of a lawsuit under federal notice standards, the facts go directly to Defendants' arguments regarding standing. *Id.* at 3. Plaintiff argues the telephone calls demonstrate that even with remedial measures such as credit watch, victims of the data breach face damages from the misuse of their information that is not solved by such partial measures. *Id.* Plaintiff argues he seeks additional relief on behalf of the putative class due to the aforementioned newly discovered facts. *Id.* Plaintiff also argues he seeks to amend the Complaint in order obviate the need for timely discovery related to personal jurisdiction. *Id.*

Defendants oppose Plaintiff's Motion to Amend and argue the Motion is a transparent last-gasp effort to add new allegations to avoid dismissal on the same grounds as another court invoked in the companion case arising out of the same events in the United States District Court for the District of Maryland: *Chambliss v. CareFirst, Inc.*, 1:15-cv-2288-RDB (D. Md.). (ECF No. 16 at 1); *See also* (ECF No. 14-1); *See also* (ECF No. 17-1). Defendants state that in *Chambliss*, following oral argument, Judge Richard D. Bennett dismissed a nearly identical complaint to Plaintiff's Complaint in this case for lack of subject matter jurisdiction because the plaintiffs lacked Article III standing. (ECF No. 16 at 1). Similarly, in *Chantal Attias, et. al v. CareFirst, Inc. et al*, 15-cv-00882-CRC the United States District Court for the District of Columbia relied

on and cited to *Chambliss* in dismissing another complaint arising from the same incident as this case for lack of subject matter jurisdiction because the plaintiffs lacked Article III standing. (ECF No. 17-1). Thus, Defendants argue Plaintiff's allegations of "new facts" change nothing, and granting Plaintiff's Motion to Amend would be futile, and would result in undue delay and prejudice to them. *Id.* at 2, 5. Defendants argue that even if the amendments were permitted, the same problems remain: (1) Plaintiff lacks Article III standing; (2) Defendants are not subject to personal jurisdiction in Illinois of Plaintiff's specific claims stemming from a data breach that occurred on Defendants' computer systems in Maryland; and (3) Plaintiff still fails to plead any plausible claims. *Id.* at 5.

Defendants argue the alleged "newly discovered" facts do not cure the lack of subject matter jurisdiction in this case because: (1) the two telephone calls do not constitute a concrete injury-in-fact and (2) Plaintiff has failed to plead a causal connection between the breach and the calls. *Id.* at 6. Defendants argue that even in cases where, unlike here, a plaintiff is a victim of actual identity theft or fraud, the alleged injury must be fairly traceable to the data breach. *Id.* Thus, Defendants argue that while the alleged April caller knew Plaintiff's address and telephone number, such information was not allegedly stolen in the breach. *Id.* Defendants argue that even if Plaintiff had originally included the "new facts" in his Complaint, he would not have Article III standing to pursue his claims against Defendants. *Id.*

Next, Defendants argue Plaintiff's allegations of phone calls allegedly made by a third party in April do not change the fact that this Court does not have personal jurisdiction over them. *Id.* at 7. Citing to their Motion to Dismiss, Defendants argue Plaintiff only makes two allegations regarding the Court's possible exercise of personal jurisdiction: (1) Defendants are "Mid-Atlantic companies that provide CareFirst health care plans to their employees all across the United States";

and (2) the Court "has personal jurisdiction over Defendant because it transacts business in this district and has such minimum contacts in this state to make this Court's exercise of jurisdiction proper." *Id.*; (ECF No. 10-1 at 10-11 (citing ECF No. 1 at 1-4)). Defendants argue conclusory allegations like this cannot establish personal jurisdiction, and even if true, they are not enough. (ECF No. 10-1 at 11). Defendants also argue they do not have the requisite minimum contacts with Illinois, and even if those contacts existed, subjecting them to jurisdiction in Illinois would offend traditional notions of fair play and substantial justice. *Id.* at 11. With respect to the proposed Amended Complaint, Defendants argue it contains additional allegations of purported contacts with Illinois, but nonetheless fails to allege the appropriate minimum contacts. (ECF No. 16 at 7). Finally, Defendants argue Plaintiff fails to plead any plausible claims for relief. *Id.* Specifically, Defendants argue Plaintiff's proposed Amended Complaint fails to add any new allegations that would save his claims from dismissal for failure to state a claim pursuant to Rule 12(b)(6). *Id.*

After review of the arguments submitted by both parties, it is clear that the issue the Court must first decide is whether Plaintiff has Article III standing. While the Court understands dismissal of a case at this stage of litigation is a rarity, it is apparent that this Court does not have subject matter jurisdiction in this case because Plaintiff lacks Article III standing. It is also clear Plaintiff tried to remedy this problem by filing the Motion to Amend and attaching the proposed Amended Complaint. Nevertheless, the Court finds Plaintiff has failed to show he suffered an actual injury-in-fact.

When looking at the first element of standing, the Supreme Court has recently ruled that when determining whether a plaintiff has standing, a "concrete" injury must be "de facto," meaning the injury must actually exist. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *as revised*

(May 24, 2016). Here, there is nothing in the Complaint to show Plaintiff has actually suffered a concrete injury. Unlike the plaintiffs in *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016) and *Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688 (7th Cir. 2015), who had standing in pertinent part because their credit card information was stolen and fraudulent charges had already occurred, the plaintiff in this case has not alleged he suffered any *present* injuries to show the risk of future harm is certainly impending. Instead, Plaintiff's Complaint contains allegations of injury that are general and conclusory at best. Particularly, the Complaint alleges:

> (1) consumers face a lifelong battle to control the damages of their PII being stolen by hackers, including fraudulent tax returns, stolen identities, and/or medical identity fraud; (2) Defendants' failure to adequately protect PII has caused, and will continue to cause, substantial customer harm and injuries to Defendants' members and employees across the United States; (3) consumers such as Plaintiff expect that part of their insurance premiums will be devoted to ensuring reasonable security of PII, Plaintiff feels stress over his loss of control over his PII and/or publication of his PII, which he fears will subject him to lifelong exposure to identity theft, medical date misuse and other repercussions; (4) due to the data breach, to date, Plaintiff has expended hours attempting to safeguard himself from identity theft or other harms caused by the release of his PII as a result of the data breach, going forward Plaintiff will have to expend effort to contain the impact of Defendants' data breach as it relates to his PII that, on information and belief, is now in the public domain; (5) as a direct and proximate result of Defendants' breach of its duties, Plaintiff and members of the Class have been harmed by the release of their PII, causing them to expend personal income on credit monitoring services and putting them at an increased risk of identity theft.

(ECF No. 1 at 3-14, ECF No. 15-1at 4-18). Thus, it is apparent Plaintiff has failed to allege an injury that is *certainly impending* to constitute an injury in fact because he has not alleged his data has been misused in anyway thus far. Instead, Plaintiff relies on allegations of future harm, and as the Supreme Court noted in *Clapper*, "allegations of *possible* future injury are not sufficient" to establish Article III standing. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013). The data breach in this case allegedly occurred on June 19, 2014, yet as of February 23, 2016, the day

the Complaint in this case was filed, Plaintiff had not suffered any fraudulent charges or other evidence of misuse as a result of the data breach.

Furthermore, while Plaintiff alleges "non-financial data is worth 10 times more than your credit card number on the black market," and "hackers are looking to steal non-financial information so they can continue to monetize victims' identities over a longer period of time," Plaintiff has failed to allege how the independent third party hacker in this situation would use his or the putative class members' stolen information for fraudulent purposes. To the extent Plaintiff relies on the "objectively reasonable likelihood" standard to assert that "once hackers have a medical ID, they can use it to procure prescription drugs or expensive medical equipment or simply to commit financial fraud," in *Clapper*, the Supreme Court held that standard to be inconsistent with the requirement that a threatened injury must be *certainly impending* to constitute injury in fact. *Id.* Moreover, as noted above, the Complaint is completely void of any allegation that Plaintiff or any of the putative class members' information has been used to commit financial fraud.

Next, with respect to Plaintiff's alleged mitigation costs due to expending personal income on credit monitoring services, the Court finds Plaintiff's allegations are insufficient to establish standing. Most notably, the Complaint "does not allege what those expenses are with any specificity, [and] [e]ven if specific expenses had been alleged, such expenses would not qualify as actual injuries under *Clapper*" because a plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, at *4 (N.D. Ill. Sept. 3, 2013); *Clapper*, 133 S. Ct. at 1151. "If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an

expenditure based on a nonparanoid fear." *Clapper*, 133 S. Ct. at 1151. Furthermore, Plaintiff has failed to plead facts to show he faces imminent or substantial risk of harm, and the information Plaintiff alleges was accessed in the data breach makes any alleged harm much less imminent than the substantial risk of harm recognized in *Remijas* and *Lewert*.

In *Remijas* and *Lewert* the time and money the plaintiffs spent for mitigation purposes was in the face of imminent harms that were recognized as cognizable injuries because the hackers in those cases accessed data that included credit cards numbers, and fraudulent charges had already occurred on the credit cards that were accessed. On the other hand, this case is more analogous to *Clapper*, wherein there is a highly speculative and highly attenuated chain of possibilities that are necessary to tie the data Plaintiff alleges was accessed in the data breach to possible misuse by the hackers that will lead to possible future injuries. Thus, similar to *Clapper*, Plaintiff's allegations are too speculative to support standing. As such, the Court finds Defendants' Motion to Dismiss must be granted.

Additionally, the Court finds that granting Plaintiff's Motion to Amend would be futile because the proposed Amended Complaint would not survive a motion to dismiss. In addition to the aforementioned allegations in the original Complaint, the proposed Amended Complaint adds the following allegations: (1) as a direct and proximate result of the misuse of data which was accessed on or around June 19, 2014, Plaintiff and his wife suffered a loss of time and money due to having to dispute and attempt to reverse unauthorized charges made on multiple different financial accounts; and (2) the April 2016 phone calls. (ECF No. 15-1 at 11-12). To support the first new allegation, Plaintiff alleges "[s]ome of these charges, fraud alerts, and various communications occurred on or around August 22, 2014; July 9, 2015; and July 21, 2015," to try to bolster his standing argument. (ECF No. 15-1 at 11). Furthermore, in his August 19, 2016,

Memorandum, Plaintiff attempts to support this allegation by alleging that on August 26, 2014, a fraudulent charge of over $5,000.00 appeared on his credit card from or through Orbitz.com; no other data breach occurred to any other company with which he dealt during the time period in question; and as a result he asserts the fraudulent charges were incurred utilizing data obtained from the CareFirst breach. (ECF No. 18 at 2-3). Nevertheless, the Court finds these attempts fail because while all of the aforementioned dates occurred before the original Complaint was filed, Plaintiff does not allege or explain how the allegedly unauthorized charges can be traced to the challenged action of Defendants, and not simply the result of an independent action of some third party not before the Court. This is an important point because nowhere in the Complaint or the proposed Amended Complaint does Plaintiff allege credit card or financial information *was* stolen.

Furthermore, with respect to the second allegation, as Defendants have correctly pointed out, Plaintiff's address and telephone number, information claimed to be used by the alleged April caller, were not sources of information Plaintiff alleges were stolen in the breach. Conversely, the Complaint alleges "hackers gained access to sensitive confidential data entrusted to Defendants, including full names, *email addresses*, dates of birth, and other personal information including user names and subscriber numbers or subscriber ids." (ECF No. 2 at 19, ECF No. 15-1 at 3). Thus, similar to the first additional proposed allegation, it is not clear how the alleged April 2016 call can be traced to the challenged action of the Defendants. As such, the Court finds the Motion to Amend must be denied because it would not survive a motion to dismiss because Plaintiff has failed to show he has Article III standing in this case. Considering the fact that Plaintiff does not have standing, this Court lacks subject matter jurisdiction over this case.

CONCLUSION

For the reasons stated above, Defendants' Motion to Dismiss (ECF No. 10) is GRANTED and Plaintiff's Motion to Amend (ECF No. 15) is DENIED. This matter is now TERMINATED.

ENTERED this 23rd day of August, 2016.

/s/ Michael M. Mihm
Michael M. Mihm
United States District Judge