CASE NO. 15-3690

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

DANIEL B. STORM, *et al.*,
Appellants

v.

PAYTIME, INC.,
Appellee

Appeal from the Orders of the United States District Court for the Middle District of Pennsylvania in Civil Action Nos. 14-1138 and 14-3964 (Jones, J.)

BRIEF OF APPELLANTS

CARLSON LYNCH SWEET & KILPELA LLP
Gary F. Lynch
Edwin J. Kilpela
Jamisen A. Etzel
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
(p) (412) 322-9243
(f) (412) 231-0246

Additional Attorneys
Listed on Inside Page

Attorneys for Appellants

April 11, 2016

LITE DEPALMA GREENBERG LLC
Katrina Carroll
211 West Wacker Drive, Suite 500
Chicago, IL 60606
(p) (312) 750-1265

LITE DEPALMA GREENBERG LLC
Mindee J. Reuben
1521 Locust Street, 7th Floor
Philadelphia, PA 19102
(p) (267) 519 8306
(f) (215) 569-0958

LOCKRIDGE GRINDAL NAUNEN PLLP
Karen H. Riebel
Eric N. Linsk
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
(p) (612) 339-6900

MEREDITH & NARINE
Joel C. Meredith
Krishna B. Narine
100 South Broad Street, Suite 905
Philadelphia, PA 19110
(p) (215) 564-5182
(f) (215) 569-0958

Attorneys for Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

I. STATEMENT OF JURISDICTION

The District Court had jurisdiction under 28 U.S.C. § 1332(d)(2) because all of Appellants' class action complaints allege claims on behalf of Appellants and other class members that exceed $5,000,000, exclusive of interests and costs, and there are numerous class members who are citizens of states other than Defendant-Appellee's state of citizenship. [JA0044 ¶ 12 (*Holt* Compl.)]; [JA0089 ¶ 12 (*Storm* Am. Compl.)]; [JA0113 ¶ 17 (CAC)].

This Court has jurisdiction under 28 U.S.C. § 1291 because Appellants' appeal stems from a final order. After the District Court dismissed Appellants' two separate complaints on March 13, 2015, without entering judgment [JA0005–06], Appellants' filed a motion for leave to file a consolidated amended complaint [JA0105-07], which the District Court denied on October 6, 2015. [JA0031-32]. Although the District Court again failed to enter a separate judgment, the order denying leave to file an amended complaint became a final, appealable order for appellate jurisdiction purposes when all Appellants elected to stand on their proposed consolidated amended complaint and timely filed a joint notice of appeal on November 3, 2015. [JA0001-04]. For further discussion of this Court's jurisdiction, see Section VII.C, *infra*.

II. STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

1. Is the allegation that Plaintiffs-Appellants' personal financial and identifying information was deliberately and successfully stolen by data thieves as part of a system-wide cyber security breach, as opposed to merely being accessed or exposed to potential theft, sufficient to create the plausibility that the misuse of such data is certainly impending, or that there is a substantial risk that misuse will occur, thereby establishing Article III standing at the pleading stage of the litigation?

Appellants addressed this issue in their brief in opposition to Paytime's motion to dismiss, *see* Case No. 14-cv-1138, ECF No. 37, and in their brief in support of their motion for leave to file an amended complaint, *see* Case No. 14-cv-1138, ECF No. 49-1. The district court ruled on the issue in both its order granting Paytime's motion to dismiss, [JA0005-27], and its order denying Appellants' motion for leave, [JA0028-34].

III. STATEMENT OF RELATED CASES AND PROCEEDINGS

This case has not been before this Court previously. Appellants are unaware of any related actions.

IV. CONCISE STATEMENT OF THE CASE

A. Facts Relevant to the Issues Raised on Appeal

At issue on appeal are three complaints: 1) Appellants Holt and Redding's (the "*Holt* Appellants") class action complaint (the "*Holt* Complaint") filed on June 27, 2014 in the Eastern District of Pennsylvania; 2) Appellants Storm, White, McMichael, and Wilkinson's (the "*Storm* Appellants") first amended class action complaint (the "*Storm* Amended Complaint") filed in the Middle District of Pennsylvania on August 8, 2014; and 3) Appellants Storm, White, McMichael, Wilkinson, Holt, and Redding's (collectively, the "Employees") first consolidated amended class action complaint (the "CAC"), which was attached to Employees' motion for leave to file the CAC that was filed in the Middle District of Pennsylvania on May 19, 2015.

This appeal concerns the Employees' standing to assert claims for the theft of their personal financial and identifying information, including their names, Social Security numbers, bank-account information, dates of birth, hire dates, wage information, home and cellular telephone numbers, home addresses, and other payroll-related information, as well as the names, Social Security numbers and dates of birth of their dependents and beneficiaries (collectively "PFI"), during a 2014 data breach of Paytime, Inc.'s ("Paytime" or "Appellee") electronic payroll records (the "Data Breach"). Paytime is a payroll service company delivering a

wide range of services, including payroll and human resource management services to thousands of businesses and individuals. [JA0041 ¶ 1 (*Holt* Compl.)]; [JA0088 ¶ 6 (*Storm* Am. Compl.)]; [JA0109 ¶ 1 and JA0111 ¶ 9 (CAC)]. Paytime came into possession of Employees' PFI, through its payroll processing and human resource management contracts with Employees' current and former employers. [JA0043-44 ¶¶ 9-10 (*Holt* Compl.)]; [JA0089 ¶¶ 14-15 (*Storm* Am. Compl.)]; [JA0114 ¶¶ 22-23 (CAC)].

All three complaints at issue on appeal assert claims against Paytime for negligence and breach of contract stemming from Paytime's failure to secure Employees' PFI and prevent the theft of Employees' PFI during the Data Breach. [JA0041-60 (*Holt* Compl.)]; [JA0087-100 (*Storm* Am. Compl.)]; [JA0109-138 (CAC)]. The *Holt* Complaint, the *Storm* Amended Complaint, and the CAC all allege that Employees' PFI was accessed between April 7, 2014 and April 30, 2014, [JA0042 ¶¶ 3-4 (*Holt* Compl.)]; [JA0088 ¶¶ 5 and JA0089 ¶¶ 16-17 (*Storm* Am. Compl.)]; [JA0110 ¶¶ 3-4, and JA0115 ¶¶ 24, 26 and 29 (CAC)], and that Employees' PFI was stolen. [JA0042 ¶ 5, JA0045 ¶ 17, JA0046 ¶¶ 19 and 22 (*Holt* Compl.)]; [JA0087 ¶¶ 1-2 and JA0090 ¶ 20 (*Storm* Am. Compl.)]; (JA0110 ¶¶ 5 and JA0115-16 ¶¶ 25, 30 and 33 (CAC)].

In addition to allegations of access and theft of Employees' PFI, the complaints also alleged that Employees were at an increased risk of harm due to

the theft of their PFI. The *Storm* Amended Complaint cited a study alleging that "nearly 1 in 4 data breach letter recipients became a victim of identity fraud." [JA0090 ¶ 23]. The *Holt* Complaint alleged that "identity thieves use personal identifying data to open financial accounts, receive government benefits, and incur charges and credit in a person's name" and that a "person whose personal information has been compromised may not see any signs of identity theft for years." [JA0047-48 ¶¶ 25-28]. The CAC incorporated all of the above allegations from the *Storm* Amended Complaint and the *Holt* Complaint, [JA0117-18 ¶¶ 36-39 and JA0120-21 ¶ 48], and also alleged that the Data Breach was orchestrated by skilled foreign hackers who intended to, and ultimately did, steal the Employees' PFI with intent to sell the information on the black market. [JA0110 ¶¶ 4 and JA0121 ¶ 49]; [JA0140 (Data Event Letter)].

After the Data Breach, Paytime offered Employees and all individuals affected by the Data Breach one year of free credit monitoring. [JA0050-51 ¶ 38 (*Holt* Compl.)]; [JA0123 ¶ 56 (CAC)]. Employees alleged that this offer is insufficient, however because Employees will have to monitor their identity for years to come as a result of the protracted nature of identity fraud risk associated with data beaches. [JA0050-51 ¶¶ 37-40 (*Holt* Compl.)]; [JA0091-92 ¶¶ 27-28 (*Storm* Am. Compl.)]; [JA0123-24 ¶¶ 55-58 (CAC)]. Appellant Redding, as a result of the Data Breach, closed her savings account, opened a new account, and

paid out-of-pocket for a fraud alert to be placed on her credit report. [JA0043-44 ¶ 10 (*Holt* Compl.)]; [JA0112-13 ¶ 16 (CAC)]. Appellant Wilkinson, also as a result of the Data Breach, was required to travel to another work location for security reasons, increasing his daily commute by four hours and causing him to incur travel expenses, as well as lost time. [JA0092 ¶ 29 (*Storm* Am. Compl.)]; [JA0123-24 ¶ 59 (CAC)].

B. Procedural History

On June 13, 2014, the *Storm* Appellants filed suit against Paytime in the Middle District of Pennsylvania. [JA0075-86]. On June 27, 2014, the *Holt* Appellants filed the *Holt* Complaint in the Eastern District of Pennsylvania, which alleged similar causes of action against Paytime relating to the Data Breach. [JA0038-60].

On August 8, 2014, Paytime filed a motion to dismiss for failure to state a claim and for lack of jurisdiction in the *Holt* action, [JA0061] and the next day, filed a motion to transfer venue and consolidate the *Holt* action with the *Storm* action in the Middle District of Pennsylvania, [JA0036, at ECF No. 6 (*Holt* Docket)]. Defendant's motion to transfer venue was granted on September 26, 2014. [JA0062-67]. The Middle District of Pennsylvania then consolidated the *Holt* and *Storm* actions on February 18, 2015. [JA0103-04].

Meanwhile, the *Storm* Appellants filed the *Storm* Amended Complaint on August 8, 2014, [JA0087-100], and Paytime filed a motion to dismiss for failure to state a claim and for lack of jurisdiction on August 27, 2014, [JA0101-02].

On March 13, 2015, by memorandum and order, the Middle District of Pennsylvania dismissed without prejudice the *Holt* Complaint and the *Storm* Amended Complaint for lack of subject matter jurisdiction. [JA0005-06]. On May 19, 2015, Employees filed a motion for leave to file the CAC. [JA0105-07]. The Employees' proposed CAC was attached as an exhibit to their motion. [JA0108-38]. On October 6, 2015, the District Court entered an order denying Employees' motion, finding that the proposed amendments would be futile. [JA0028-34].

On November 3, 2015, Employees filed a joint notice of appeal of the District Court's March 13, 2015, memorandum and order granting Paytime's motion to dismiss the *Holt* Complaint and the *Storm* Amended Complaint, as well as the District Court's October 6, 2015 order denying Employees' motion for leave to file the CAC. [JA0001-04].

V. SUMMARY OF ARGUMENT

Employees suffered an injury-in-fact when their sensitive information was stolen—from an entity trusted to hold it—by skilled thieves who deliberately stole the information and intended to misuse it. Victims of that type of data breach, like Employees here, have standing to attempt to prove negligence on the part of the

data holder and to seek redress for the substantial risk of harm and any realized harm which stems from that alleged negligence.

All three of Employees' complaints alleged that Employees faced a substantial risk of future harm because the PFI was stolen during a breach of Paytime's electronic payroll records. Employees alleged that their PFI was stolen by "skilled" and "dedicated thieves" who intended to misuse Employees' PFI. Employees also cited studies to support their allegation that when certain PFI is stolen, the data breach victims are at a significantly increased risk of fraud and identity theft compared to the general population. Under well-established principles of standing—and also several recent opinions in factually analogous cases—Employees' allegations sufficed to demonstrate an Article III injury-in-fact.

The Seventh Circuit recently found that data breach victims who alleged that their PFI was stolen deliberately by hackers had standing to bring negligence claims against the corporation that had stored the plaintiffs' data. In *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692-96 (7th Cir. 2015), the Court found that the Article III injury-in-fact requirement was met because there was no need to speculate whether the plaintiffs' information was stolen and that sensitive PFI was stolen. The plaintiffs' allegations of deliberate theft made it plausible to infer that the plaintiffs faced a substantial risk of harm from the breaches, and the *Remijas* court held that they had no further burden at the pleading stage.

The opinion in *Remijas* cited with approval and closely followed the reasoning of a California district court in *In re Adobe Sys. Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1212-16 (N.D. Cal. 2014). In that case, the named plaintiffs did not allege that any of them had suffered misuse of their appropriated data, but they did allege that the hackers had used stolen data for other purposes, such as using stolen information to decrypt credit card numbers and to discover vulnerabilities in Adobe software products. From these allegations, *Adobe* court found that the prospect that the plaintiffs' stolen data would be misused was "certainly impeding" and posed a substantial risk of future harm sufficient to support standing. The *Adobe* court noted that if it were to require the data breach victims to wait until they had actually suffered identity theft, such a holding would run counter to well-established principles of standing and would set the bar for establishing injury-in-fact impermissibly high.

These opinions are consistent with the Supreme Court's recent confirmation, in at least two cases, that an injury-in-fact need not be literally certain to confer standing so long as the threatened injury is certainly impending *or* there is a substantial risk that the future harm will occur. The Supreme Court continues to recognize that damages *do not* need to have already occurred before the plaintiff can file an action. Indeed, a long line of cases hold that at the pleading stage, the plaintiff's burden to establish standing is distinct from the plaintiff's burden to

prove damages in order to succeed on the merits of the plaintiff's claim. The standing inquiry is not meant to shift the plaintiff's burden of proving damages to an earlier stage of the litigation.

The District Court erred in this regard and incorrectly applied *Clapper v. Amnesty Intern. USA*, 133 S.Ct. 1138 (2013) by improperly requiring Employees to pass a higher threshold and allege that they had already suffered actual identity theft. As numerous courts have since held, *Clapper* did not alter the pleading requirements pertinent to standing, and *Clapper* is also distinguishable due to its unique facts. The District Court misapplied *Clapper* by prematurely evaluating the merits of Employees' allegations with respect to the substantial risk of future harm that they faced, by failing to credit Employees' allegations as true, and also by overemphasizing the fact that Employees had not pled any incidents of actual identity theft.

The District Court concluded that a year and a half after the data breach, "there is still no sign" of identity theft among the Employees, but this observation was inappropriate for two reasons. First, Employees should not have been required to allege that they had already suffered identity theft at the outset of litigation, especially since Employees also alleged that instances of identity theft can continue to emerge for years after a data breach. Second, Employees did not have an opportunity to show evidence of the present incidence of identity theft among

the proposed class because Employees' complaints were dismissed before any class certification proceedings were held or any discovery was taken.

Finally, this Court's opinion in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) did not require dismissal, as the District Court thought, and this Court does not need to overturn *Reilly* in order to reverse the District Court here. The facts of *Reilly* are distinguishable because the plaintiffs there *did not* allege that the hackers who infiltrated the defendant's data systems were in fact able to access the plaintiffs' sensitive information; nor did the *Reilly* plaintiffs allege that the hackers read, copied, or understood the potentially accessed data or intended to steal the data for nefarious purposes. This Court was unable to conclude that the *Reilly* plaintiffs had standing because their supposed injury-in-fact was entirely theoretical; the plaintiffs could not show a substantial risk of future harm because they relied on mere speculation that their data had even been stolen, and even more speculation that it had been stolen by someone who had the intent and ability to use the stolen information to the plaintiffs' detriment. By contrast, Employees alleged that skilled hackers stole their PFI from Paytime with the intent and ability to misuse the data and sell it on the black market. Therefore, the chain of hypotheticals that the *Reilly* plaintiffs were forced to rely on to demonstrate standing is simply not present in this case.

VI. STANDARD OF REVIEW

A Rule 12(b)(1) motion to dismiss challenges a court's subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). This Court exercises "plenary review of a District Court's dismissal for lack of subject matter jurisdiction." *U.S. ex rel. Atkinson v. PA. Shipbuilding Co.*, 473 F.3d 506, 514 (3d Cir. 2007). A facial attack on subject matter jurisdiction restricts a court's focus to the allegations in the pleadings and requires the court to view the allegations in the light most favorable to the plaintiff. *Id.* A facial attack "concerns an alleged pleading deficiency whereas a factual attack concerns the actual failure of a plaintiff's claims to comport factually with the jurisdictional prerequisites." *CNA v. U.S.*, 535 F.3d 132, 139 (3d Cir. 2008), as amended (Sept. 29, 2008) (quotation marks and alterations omitted). Here, Paytime's attack was facial because it concerned only the sufficiency of Employees' allegations. As such, the Court must accept as true all of Employees' allegations and make all inferences reasonably deduced therefrom in favor of Employees.

VII. ARGUMENT

A. A Substantial Risk of Future Harm Qualifies as an Article III Injury-in-Fact

"Article III of the Constitution limits the jurisdiction of federal courts to 'Cases' and 'Controversies.'" *Susan B. Anthony List v. Driehaus*, 134 S.Ct. 2334, 2341 (2014) (quoting U.S. Const., Art. III, § 2). The doctrine of "Article III standing enforces th[is] case-or-controversy requirement." *Daimler Chrysler Corp. v. Cuno*, 547 U.S. 332, 342 (2006) (alterations omitted). "To establish Article III standing a plaintiff must show (1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision." *Driehaus*, 134 S.Ct. at 2341 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)) (quotation marks and alterations omitted). Although the "party invoking federal jurisdiction bears the burden of establishing standing…, [e]ach element must be supported…[only to] the matter and degree [] required at the successive stages of the litigation." *Id.* at 2342. "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss [courts must] presume that general allegations embrace those specific facts that are necessary to support the claim." *Lujan*, 504 U.S. at 561 (alterations and quotation marks omitted).

This case concerns Article III's "injury-in-fact" requirement, which simply requires allegations of "some specific, 'identifiable trifle' of injury." *Bowman v. Wilson*, 672 F.2d 1145, 1151 (3d Cir. 1982). An Article III injury-in-fact "must be concrete and particularized and actual or imminent, not conjectural or hypothetical," *Driehaus*, 134 S.Ct. at 2341 (quotation marks omitted), but it need not be "literally certain" to confer standing. *Clapper*, 133 S.Ct. at 1150 n. 5. For example, allegations of future injury satisfy Article III's injury-in-fact requirement so long as 'the threatened [future] injury is certainly impending, *or* there is a substantial risk that the [future] harm will occur.'" *Driehaus*, 134 S.Ct. at 2431 (emphasis added) (quotations marks omitted); *Neale v. Volvo Cars of N.A., LLC*, 794 F.3d 353, 359 (3d Cir. 2015) (same); *see, e.g.*, *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153 (2010); *see also* 7 AA CHARLES ALAN WRIGHT, ARTHUR R. MILLER, MARY KAY KANE, FED. PRAC. & PROC. CIV. 3d § 1785.1 (2005) ("If [a] plaintiff can show that there is a possibility that [the] defendant's conduct may have a future effect, even if injury has not yet occurred, the court may hold that standing has been satisfied."). Indeed, an Article III injury-in-fact "may simply be the fear or anxiety of future harm" or may "entail economic costs" incurred to prevent future harm. *Denney v. Deutsche Bank AG*, 443 F.3d 253, 264-65 (2d Cir. 2006).

Importantly, an Article III injury-in-fact supporting a plaintiff's ability to be heard in court, is distinct from the injury a plaintiff must establish to prove a claim. *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990) ("Our threshold inquiry into standing in no way depends on the merits of the [plaintiff's claim.]"); *Assn. of Data Processing Serv. Organizations, Inc. v. Camp*, 397 U.S. 150, 153 (1970) (stating that merits question and standing inquiry are different). In fact, a plaintiff may satisfy Article III's injury-in-fact requirement, and simultaneously fail to state a valid cause of action. *See Denney*, 443 F.3d at 264 (stating that "injury-in-fact need not be capable of sustaining a valid cause of action" and finding that "future-risk members of the Denney class have suffered injuries-in-fact, irrespective of whether their injuries are sufficient to sustain any cause of action"); *see, e.g.*, *Pisciotta v. Old Nat. Bancorp.*, 499 F.3d 629 (7th Cir. 2007) (finding standing to assert data breach claims, but finding that those claims did not state a valid cause of action).

In sum, Article III's injury-in-fact requirement "is not Mount Everest," *Danvers Motor Co., Inc. v. Ford Motor Co.*, 432 F.3d 286, 294 (3d Cir. 2005); *see also Ross v. Bank of Am., N.A.(USA)*, 524 F.3d 217, 222 (2d Cir. 2008) (stating Article III's injury-in-fact requirement "is a low threshold"), and is readily satisfied when the plaintiff's complained of injury is personal to him and ensures he has a direct stake in the litigation, *see U.S. v. Students Challenging Reg. Agency*

Procedures, 412 U.S. 669, 690 n. 14 (1973) (stating Article III "'[i]njury in fact'…serves to distinguish a person with a direct stake in the outcome of a litigation—even though small—from a person with a mere interest in the problem.").

B. The *Storm* Amended Complaint, the *Holt* Complaint and the CAC Allege Article III Injury-in-Fact

i. The District Court Ignored and Disregarded Allegations that Establish Article III Injury-in-Fact

A plaintiff may establish standing to litigate a negligence claim by alleging that the plaintiff is at a substantially increased risk of identity theft because a hacker stole the plaintiff's sensitive personal and financial information from the defendant for nefarious purposes. *Remijas*, 794 F.3d at 692-96 (plaintiffs suffered Article III injury-in-fact when personal information stolen by hackers in data breach); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141-43 (9th Cir. 2010) (same); *Pisciotta*, 499 F.3d at 634 (same); *Adobe*, 66 F. Supp. 3d at 1212-16 (same); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014) (same).

On this point, *Remijas* and *Adobe* are instructive. In those cases, like here, the plaintiffs alleged that hackers deliberately targeted and stole their personal information. *Remijas*, 794 F.3d at 692, 693; *Adobe*, 66 F. Supp. 3d at 1206, 1214-15. As these allegations were required to be taken as true, there was "no need to

speculate as to whether [the plaintiffs'] information had been stolen and what information was taken." *Remijas*, 794 F.3d at 693 (citing *Adobe* 66 F. Supp. 3d at 1215) (alteration and quotation marks omitted). The plaintiffs' allegations of theft, at the pleading stage, made it "plausible to infer that the plaintiffs ha[d] shown a substantial risk of harm" stemming from the respective date breaches—"[w]hy 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 fraudulent charges or assume those consumers' identities.*" *Id.* (emphasis added); *Adobe*, 66 F. Supp. 3d at 1216 (similar).

The *Remijas* court also recognized that the plaintiffs' complaint—which cited the same United States Government Accountability Office Report (the "GAO Report") cited by Employees here—"assert[ed] that fraudulent charges and identity theft can occur long after a data breach." *Remijas*, 794 F.3d at 694. Although it was possible that the assertions contained in the GAO Report may not provide a factual basis for the plaintiffs' standing down the road, the Seventh Circuit stated that the plaintiffs "had no such burden at the pleading stage," and that "[t]heir allegations of future injury [were] sufficient to survive a 12(b)(1) motion." *Id.*; *see also Sutton v. St. Jude Med. S.C., Inc.*, 419 F.3d 568, 575 (6th Cir. 2005) ("Though the plaintiffs in [another case] were able to demonstrate a 700–percent increase in risk associated with using the heart valves there at issue, we hold it unnecessary for

a plaintiff to make such a showing as a matter of course. Such a vast increase in the risk of injury clearly establishes an injury in fact, but to require a plaintiff to so clearly demonstrate her injury in order to confer standing is to prematurely evaluate the merits of her claims. Here [the plaintiff] alleges an increased risk of harm when comparing those individuals implanted with the device to those undergoing traditional surgery. Accepting [the plaintiff's] allegations as true, the standing requirements have been met.").

Here, similar to *Remijas* and *Adobe*, the three complaints at issue alleged that Employees' personal information was stolen, and that this theft subjected them to a substantial risk of harm.

The *Holt* Complaint alleged that hackers accessed, stole and continue to use the PFI of the *Holt* Plaintiffs. [JA0042 ¶¶ 3-5, JA0045 ¶ 17, and JA0046 ¶¶ 19 and 22]. The *Holt* Complaint then alleged that this put the *Holt* Plaintiffs at a substantial risk of identity fraud because the GAO Report shows that harm can occur years after a person's data is stolen. [JA0047-48 ¶¶ 25-28]. The *Storm* Amended Complaint also alleged that hackers accessed and stole the PFI of the *Storm* Plaintiffs. [JA0087 ¶¶ 1-2, JA0088 ¶ 5, JA0089 ¶¶ 16-17 and JA0090 ¶ 20]. The *Storm* Amended Complaint then alleged that this put the *Storm* Plaintiffs at a substantial risk of identity fraud because one in four persons who are the victims of a data breach go on to become victims of identity fraud. [JA0090 ¶ 23]. The

allegations of theft and an increased risk of harm in these complaints are sufficient to establish Article III injury-in-fact.

The CAC also alleged Article III injury-in-fact. The CAC alleged that Employees' PFI was accessed for almost a month [JA0110 ¶¶ 4, and JA0114 ¶¶ 24, 26-27 and 29], that Employees' PFI was stolen during that time, [JA0110 ¶ 5, and JA0115-16 ¶¶ 25, 30 and 33], that hackers continue to use Employees' PFI, [JA0110 ¶ 5, and JA0115 ¶ 30], and that the theft of Employees' PFI was completed by "skilled" and "dedicated thieves" who seek to misuse Employees' PFI, [JA0110 ¶ 4, and JA0121 ¶ 49]; [JA0140 (Data Event Letter)]. The CAC then alleged that this theft has subjected Employees to a substantial risk of harm. [JA0117-18 ¶¶ 36-39, and JA0121 ¶ 48]. Employees cited the GAO Report for the proposition that identity fraud takes time to manifest after a person's personal information is stolen, and that it may take years for a data theft victim to suffer injury. [JA0117-18 ¶¶ 36, 38-39]. Employees also cited the overview of a 2013 Identity Fraud Report released by Javelin Strategy & Research (the "Javelin Report"), which states that "nearly 1 in 4 data-breach letter recipients became a victim of identity fraud." [JA0121 ¶ 48]. Importantly, this figure does not equate to a 25% increase in the risk of identity fraud. As the overview of the 2013 Javelin Report makes clear, 5.26% of United States adults suffered identify fraud in 2012, while nearly 25% of those victimized by data breaches suffered identify fraud,

meaning data breach victims have an almost 400% increased risk in being victimized by identity fraud. (Javelin Strategy & Research, *Overview, 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*,[1] [cited at JA0121 ¶ 48 n. 16]. Moreover, the study found that consumers who had their Social Security numbers compromised, like Employees here, were 5 times more likely to be a fraud victim than the average consumer (which equates to a 500% increase in the risk of identity fraud). (*Id.*). These allegations confirm that the theft of Employees' PFI subjects them to a substantial risk of future identity fraud, and that this risk last for years after the data breach. Accordingly, the CAC's allegations establish Article III injury-in-fact.

The District Court failed to take Employees' allegations as true. In fact, in both Orders at issue on appeal, the District Court engaged in fact-finding with respect to the degree of Employees' risk of future injury. In its order dismissing the *Holt* Complaint and *Storm* Amended Complaint it stated: "even though [Employees] may indeed be at a greater risk of identity theft, the data breach in this case occurred in April 2014—almost a year ago—and [Employees] have yet to allege that any of them have become actual victims of identity theft. Indeed, putting aside the legal standard for imminence, a layperson with a common sense

[1] The overview of the report is available at http://www.javelinstrategy.com/brochure/276.

notion of 'imminence' would find this lapse of time, without any identity theft, to undermine the notion that identity theft would happen in the near future." [JA0022]. The District Court repeated this logic in its order denying Employees' motion for leave: "The Court is aware that there is indeed some possibility that some of the victims of this data breach will at some future point experience an injury in the form of identity theft or fraudulent payments. However, on the fact of the [CAC] it appears that no plaintiff has experienced such injury or faces an 'immediate' risk of such injury. Moreover, the immediacy of future injury is undermined by the fact that this data breach occurred in April 2014, a year and [a] half ago, and yet there is still no sign of a single incident of identity theft among the [Employees] or proposed class." [JA0034].

The District Court's holdings were improper because they were determinations of the merits of Employees' allegations before Employees had a chance to engage in discovery and produce evidence in support of their contentions. Although Employees "may eventually not be able to provide an adequate factual basis for th[ese] inference[s], [] they have no such burden at the pleading stage." *Remijas*, 794 F.3d at 694; *see also Sutton*, 419 F.3d at 575.

In *Remijas*, the Seventh Circuit, in line with Employees' position, held that the district court prematurely terminated the plaintiffs' case by deciding the merits of the plaintiffs' contention that identity fraud can occur long after a breach, and

instructed the district court, on remand, to "look into the length of time that a victim is truly at risk." 794 F.3d at 694. The Sixth Circuit in *Sutton* similarly held that a district court prematurely evaluated the merits of the plaintiff's claims when it dismissed the plaintiff's suit on standing grounds because the plaintiff failed to clearly demonstrate how she was at an increased risk of future harm. 419 F.3d 568. The *Sutton* court stated that the plaintiff's allegations of "an increased risk of harm when comparing those individuals implanted with the [defective medical] device to those undergoing traditional surgery" were sufficient at the pleading stage to establish standing. *Id.* at 575.

Here, Employees' allegations, like those in *Remijas* and *Sutton*, establish standing and entitle Employees to discovery to prove their contentions. It may be the case that Employees ultimately are unable to prove damages. Determination of that, however, is premature at this stage of the proceeding. The District Court's decision based on its on value judgments regarding the validity of Employees' case was premature. Accordingly, Employees' allegations of theft of their PFI are sufficient to establish Article III injury-in-fact, and confer Article III standing.

Furthermore, Employees' expenses and time associated with protecting themselves from the theft and misuse of their information also confer standing. Although plaintiffs cannot manufacture standing "merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly

impending," *Clapper*, 133 S.Ct. at 1151, "it is important not to overread *Clapper*." *Remijas*, 794 F.3d at 694. If the future harm being mitigated is itself imminent or there is a substantial risk that it will occur, costs incurred in an effort to mitigate the risk constitute an injury-in-fact. *Adobe*, 66 F. Supp. 3d at 1217; *Remijas*, 794 F.3d at 694; *cf. Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 162-65 (1st Cir. 2011).

Here, as demonstrated above, the threat of future harm was imminent and Employees were at a substantial risk of identity theft. Indeed, the fact that Paytime cautioned Employees and others to take preventative measures, and itself provided free credit monitoring, evidence this substantial and imminent risk. *See Remijas*, *794* F.3d at 694 ("It is telling…that [the defendant] offered one year of credit monitoring and identity-theft protection to all customers [affected by the data breach]….It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded."). Because the risk of future injury was substantial and imminent, the mitigation costs that Appellants Redding and Wilkinson incurred give them standing in this matter. Accordingly, the District Court was incorrect in finding that Appellants Redding and Wilkson did not have standing for this additional reason.

ii. The District Court Misapplied *Clapper v. Amnesty Int'l USA*

In its original order dismissing the *Storm* and *Holt* Complaints, the District Court stated that a future injury only supports an Article III injury-in-fact when it is "certainly impending to constitute an injury in fact." [JA0017]. The District Court then cited *Clapper* for this proposition, and stated that "[t]his standard establishes a high bar for plaintiffs seeking to recover for injuries which have not in fact occurred, even if they appear likely or probable." [JA0017]. The District Court repeated this interpretation in its Order denying Employees' motion for leave to file. [JA0030] (stating that a plaintiff does not have standing unless the plaintiff "alleges actual misuse of the information or that such misuse is imminent") (quotation marks omitted); [JA0031] ("We still fail to see an actual or imminent injury alleged which would create standing."). This interpretation of *Clapper* is incorrect.

Clapper, a case decided on summary judgment (meaning the plaintiffs were required to provide factual evidence, rather than mere factual allegations, in support of their standing), involved the standing of human rights organizations (the "HROs") to challenge the federal government's surveillance activities pursuant to the Foreign Intelligence Surveillance Act ("FISA"). 113 S.Ct. at 1142, 1145-46. The Supreme Court found that the HROs did not have standing to challenge the government's FISA activities because the HROs could not show that any of their

communications were intercepted pursuant to the government's FISA authority, or that the government even was attempting to target the HROs' communications using its FISA authority. *Id.* at 1147-48. The plaintiffs' speculation and hypotheses regarding the interception of their communications simply were insufficient to establish Article III injury-in-fact. *Id.* at 1148-49.

The *Clapper* decision explicitly cautioned that plaintiffs are not required "to demonstrate that it is literally certain that the harms they identify will come about. 133 S.Ct. at 1150 n. 5. Indeed, the Supreme Court stated, "[i]n some instances…standing [is established] 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.* Since *Clapper*, the Supreme Court again made clear that allegations of future injury are sufficient to qualify as Article III injuries in fact so long as "the threatened [future] injury is certainly impending, *or* there is a substantial risk that the [future] harm will occur." *See Driehaus*, 134 S.Ct. at 2341 (emphasis added) (quotations marks omitted). This Court too has recognized that future injury satisfies Article III's injury-in-fact requirement when the "threatened harm is certainly impending *or* there is a substantial risk that the harm will occur." *Neale*, 794 F.3d at 359 (emphasis added) (quotation marks omitted); *see also Remijas*, 794 F.3d at 693 ("*Clapper* does not, as the district court thought, foreclose any use whatsoever of future injuries to support Article III standing.").

The District Court seemed to discount the fact that a substantial risk of harm could qualify as an Article III injury-in-fact. In its original memorandum explaining the dismissal the *Storm* and *Holt* Complaints, the District Court stated "we choose to rely on the [certainly impending] standard the [Supreme] Court relied on for its holding in *Clapper*, rather than [*Clapper*'s fifth] footnote," which set forth the substantial risk standard. [JA0017, n.4]. To the extent the District Court disregarded the substantial risk of harm suffered as a result of the theft of Employees' PFI, it erred as a matter of law and its ruling should be reversed.

Further, so far as the District Court relied on the facts of *Clapper* to dismiss this case it was mistaken. As the Seventh Circuit observed, the theory of injury posed by the *Clapper* plaintiffs was highly attenuated, and distinguishable from that of the *Remijas* plaintiffs and Employees here:

> Unlike in *Clapper*, where [the] 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 [plaintiff-appellants'] personal data will be misused by the hackers who breached [defendant-appellee's] network is immediate and very real….Whereas in *Clapper*, there was no evidence that any of respondents' communications either had been or would be monitored, in [this] case there is no need to speculate as to whether [plaintiff-appellants'] information has been stolen and what information was taken.

Remijas, 794 F.3d at 693 (quotation marks, citations and alterations omitted).

Finally, to the extent the District Court did apply the substantial risk standard, its application was incorrect. The District Court stated that Employees failed to plead a substantial risk of future harm because they alleged that "nearly 1 in 4 data breach letter recipients became a victim of identity theft fraud," and that "[a] 25% chance of [Employees] becoming identity fraud victims is not a substantial risk." [JA0017]. This analysis is premature and misconstrues the import of Employees' allegations.

First, the District Court's analysis prematurely evaluated the merits of Employees' claims rather than taking them as true. Employees alleged that their information was targeted and stolen, and that, as a result of this theft, they are at an increased risk of future identity fraud for years to come. These allegations must be taken as true at the pleading stage. *Lujan*, 504 U.S. at 561. If taken as true, Employees clearly alleged a substantial risk of future harm: skilled hackers who targeted their PFI now are in possession of—and using and selling—Employees' PFI. The exact degree to which Employees' risk of identity theft has increased is a factual question inappropriate for disposition on the pleadings.

Second, the District Court's analysis misinterpreted Employees' allegations. As stated in section VII.B.i. *supra*, the "nearly 1 in 4" allegation actually equates to an almost 400% increase in risk of identity fraud, and the overview of the Javelin Report cited in the CAC specifically states that persons whose Social

Security numbers are stolen have an (approximately) 500% increase in the risk of identity fraud. In any event, plaintiffs are not required to quantify their risk of increased harm at the pleading stage. *See Sutton*, 419 F.3d at 575. Employees' allegations of being at an increased risk of identity fraud because hackers who targeted their PFI have stolen it and now are in possession of, and using it, are sufficient at the pleading stage.

In sum, the District Court misconstrued *Clapper*, and even if it did not, misapplied *Clapper* to the facts of this case, and its ruling should be reversed as a result.

iii. The District Court Misapplied This Court's Holding in *Reilly v. Ceridian Corp.*

In its original order dismissing the *Storm* and *Holt* Complaints, the District Court held that *Reilly v. Ceridian Corp.*, requires district courts sitting in the Third Circuit "to dismiss data breach cases for lack of standing unless the plaintiffs allege actual misuse of the hacked data or specifically allege how such misuse is certainly impending." [JA0019]. The District Court restated its interpretation of *Reilly* in its Order denying Employees' Motion for Leave to File. [JA0030]. The District Court—in both its order of dismissal and order denying leave to file an amended complaint—held that Employees failed to allege how their risk of harm attendant to the data breach was imminent. [JA0022-23 (Order Dismissing *Holt* and *Storm* Compls.)]; [JA0031-32 (Order Denying Mot. for Leave)]. Specifically,

the District Court stated that Employees failed to allege any facts showing that they were at an increased risk of harm in this case. [JA0031-32 (Order Denying Mot. for Leave)]; [JA0022-23 (Order Dismissing *Holt* and *Storm* Compls.)]. Aside from incorrectly interpreting *Reilly* so as to disregard the substantial risk standard set forth in *Clapper*, *Dreihaus*, and this Court in *Neale*, the District Court's reliance on *Reilly* is also misplaced because that case contains material factual differences that render its holding inapplicable to this case.

In *Reilly*, the plaintiffs alleged that hackers infiltrated the defendant's data system and *potentially* gained access to the plaintiffs' personal information and the personal information of approximately 27,000 employees of various companies. *Reilly*, 664 F.3d at 40. The appellants *did not* allege that the hacker read, copied or understood the data. *Id.* In fact, taking the plaintiffs' allegations as true, this Court could only infer that "a firewall was penetrated." *Id.* at 44.

The plaintiffs in *Reilly* were found to not have standing because the plaintiffs' Article III injury-in-fact (*i.e.*, their increased risk of future identity fraud) was based on something that may not even have happened to some or all of the plaintiffs. The plaintiffs did not allege that the hacker stole, or was in possession of, their personal information, but rather, based on the fact that the defendant's data systems had been breached, speculated that theft had occurred. *Id*. at 42-46. In considering the sufficiency of these allegations, this Court noted

that most courts considering "whether the 'risk of future harm' posed by [a] data security breach[] confers standing on [a] person[] whose information *may* have been accessed…have held that such plaintiffs lack standing because the harm is too speculative." *Id.* at 43 (emphasis in original).[2] It then stated: "We agree with the holdings in those cases. Here no evidence suggests that the data has been—*or will ever be*—misused….Appellants' allegations of an increased risk of identity theft resulting from a security breach are therefore insufficient to secure standing." *Id.* (emphasis added).

This Court also distinguished the facts and reasoning of *Pisciotta*, 499 F.3d 629, a data breach case in which sophisticated hackers intentionally and maliciously hacked a defendant's data systems, and *Krottner*, 628 F.3d 1139, a data breach case in which a laptop containing personal information was stolen.

[2] In support of this proposition *Reilly* cited *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046 (E.D. Mo. 2009) and *Key v. DSW Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006). In *Amburgy*, the "plaintiff d[id] not claim that his personal information ha[d] in fact been stolen and/or his identity compromised. Rather, [the] plaintiff surmise[d] that, as a result of the security breach, he face[d] an increased risk of identity theft at an unknown point in the future." 671 F. Supp. 2d at 1052. Similarly, in *Key*, the plaintiff failed to allege theft and the court distinguished the plaintiff's case on this basis. 454 F. Supp. 2d at 691 ("Analogizing, *Sutton* would have been a more proper comparison, if the [p]laintiff's identity was actually stolen and misused. Thus, the plaintiff injury's in *Sutton*, based on distinguishable facts, was 'actual and imminent,' unlike [the p]laintiff's injury here.").

Reilly, 664 F.3d at 43-46. First, the facts of those cases did not align with the facts presented in *Reilly*:

> [I]n *Pisciotta* and *Krottner*, the threatened harms were significantly more imminent and certainly impending than the alleged harm here. In *Pisciotta*, there was evidence that the hacker's intrusion was sophisticated, intentional and malicious. In *Krottner*, someone attempted to open a bank account with a plaintiff's information following the physical theft of the laptop. Here, there is no evidence that the intrusion was intentional or malicious. Appellants have alleged no misuse, and therefore, no injury. Indeed, no identifiable taking occurred; all that is known is that a firewall was penetrated. Appellants' string of hypothetical injuries do not meet the requirement of an actual or imminent injury.

Id. at 44 (quotation marks, citations and alterations omitted). Second, the reasoning of those cases, which relied on analogizing data breach cases to defective medical-device and toxic exposure cases, was incongruent with the *Reilly* plaintiffs' allegations. Allegations of future harm are sufficient in defective medical-device and toxic tort cases because "the damage has been done; we just cannot yet quantify how it will manifest itself." *Id.* at 45. For example, "[i]n medical-device cases, a defective device has been implanted into the human body with a quantifiable risk of failure." *Id.* "Similarly, exposure to toxic substances causes injury; cells are damaged and a disease mechanism has been introduced." *Id.* By contrast, the *Reilly* plaintiffs failed to allege a quantifiable risk of future injury because their allegations merely speculated as to whether their information

was stolen, and thus, the plaintiffs' risk of future injury was hypothetical, rather than actual or real. *Id.* ("Any damages that may occur here are entirely speculative and dependent on the skill and intent of the hacker.").

These distinctions are important in understanding why *Reilly* is inapplicable here. Employees have alleged that Paytime suffered a data breach at the hands of malicious criminals, *and* that Employees' PFI was stolen. As stated in section VII.B.i. *supra*, the theft of Employees' PFI causes injury sufficient to establish Article III injury-in-fact. Similar to medical-device and toxic exposure cases, the damage has been done—malicious third parties, who targeted and understood Employees' PFI have stolen, and now are in possession of, and using, that information. The fact that the hackers may never use Employees' PFI to commit identity fraud, or that the hackers may be unsuccessful, is of no moment. For instance, in the context of defective medical device and toxic exposure cases, the plaintiff may never suffer a device malfunction or a harmful mutation manifesting disease, yet the possibility of future harm is actual, real and quantifiable. Similarly, because hackers who intended to steal Employees' PFI now possess and are using that information, the possibility of future harm certainly is present, actual, real, and quantifiable, even if that possibility may never materialize. The *Reilly* plaintiffs' possibility of future harm was conjectural and hypothetical because they failed to allege facts establishing that a substantial risk of future harm

even existed, as that possibility depended on whether their information was recognized or stolen in the first place. By contrast, the possibility of future harm is a reality in this case because Employees' PFI is in the hands of hackers who intended to steal and misuse that information. Accordingly, Employees' allegations distinguish this case from *Reilly* and the District Court was wrong to dismiss this case through application of the *Reilly* decision.

The District Court's flawed reliance on *Reilly* is magnified by the cases the District Court cited in support of dismissing the *Storm* and *Holt* Complaints and Employees' CAC. [JA0023 at 17]. For example, *In re Science Applications Int'l Corp. ("SAIC") Backup Tape Data Theft Litig.*, involved a thief who broke into a car and stole a GPS device, stereo and encrypted data tapes containing the personal information of over four million persons. 45 F. Supp. 3d 14, 20-21 (D.D.C. 2014). The *SAIC* court denied standing because it was unclear if the thief even knew what the data tapes were, or had the capability of unencrypting the data they contained. Id. at 25. Here, by contrast, the hackers targeted Employees' PFI and stole it, meaning they knew what they had found and were able to take it. *Polanco v. Omnicell, Inc.*, is equally inapplicable because in that case the plaintiff alleged that a thief stole laptop from a car, but failed to allege that the thief targeted the laptop for the information contained therein or that the thief appreciated the information the laptop held. 988 F. Supp. 2d 451, 456, 467 (D.N.J. 2013). Finally, the *Stautins*

v. Trustwave Holdings, Inc., decision refused to take the plaintiff's factual allegations of theft as true, and through its own fact finding held that theft had not occurred. 27 F. Supp. 3d 871, 879-82 (N.D. Ill. 2014). This Court should not follow *Strautins*, and, instead, should take Employees' allegations of theft as true. *Lujan*, 504 U.S. at 561.

In sum, *Reilly*'s facts are distinguishable from this matter, making its reasoning regarding Article III injury-in-fact inapposite to the disposition of this case. The District Court incorrectly applied *Reilly* in dismissing the *Holt* and *Storm* Complaints and in denying leave to file the CAC. Accordingly, its rulings should be reversed and this case remanded for further proceedings.

C. Employees Properly Appealed the District Court's Decisions

In their November 20, 2015 submission to this Court's Clerk,[3] Employees stated that they intended to stand on the proposed CAC attached to their motion for leave, and explicitly renounced any intent to reinstate the litigation. These statements make the District Court's October 6, 2015 Order final and appealable. Accordingly, appellate jurisdiction is secure because Employees timely filed their Joint Notice of Appeal within 30 days following the October 6, 2015 final Order.

[3] Employees' November 20, 2015 submission was filed in response to the Court's November 6, 2015 Order directing Employees to address whether they are standing on the complaints previously filed in the District Court.

i. The October 6, 2015 Memorandum and Order is Final Within the Meaning of 28 U.S.C. § 1291

Employees' intention to stand on their proposed CAC makes the District Court's October 6, 2015 Order denying Plaintiffs' motion for leave a final and appealable order.

Federal appellate courts "have jurisdiction of appeals from all final decisions of the district courts of the United States…." 28 U.S.C. § 1291. "A decision is considered final for purposes of § 1291 when the District Court's decision 'ends the litigation on the merits and leaves nothing for the court to do but execute the judgment.'" *Berke v. Bloch*, 242 F.3d 131, 134 (3d Cir. 2001) (quoting *Quackenbush v. Allstate Ins. Co.*, 517 U.S. 706, 710-11 (1996)). Following this standard, the Third Circuit has held that an otherwise non-appealable interlocutory order may become final and appealable when the "party seeking relief renounces any intention to reinstate litigation." *Id.* at 135; *see also Bethel v. McAllister Bros., Inc.*, 81 F.3d 376, 381 (3d Cir. 1996) ("[W]e observe that it is well established that otherwise non-appealable orders may become appealable where circumstances foreclose the possibility of piecemeal litigation."). For example, a plaintiff can convert a non-appealable dismissal without prejudice into a final order by electing to stand on the original complaint because the plaintiff's election forecloses the possibility of further litigation on the merits and leaves nothing for the court to do but execute the judgment. *In re Westinghouse Sec. Litig.*, 90 F.3d 696 (3d Cir.

1996) (quoting *Shapiro v. UJB Financial Corp.*, 964 F.2d 272, 278 (3d Cir. 1992)); *cf. Hall v. Pennsylvania State Police*, 570 F.2d 86, 88–89 (3d Cir. 1978) (acknowledging that a plaintiff can elect to stand on a proposed amended complaint). Paytime itself acknowledges that this is, indeed, the operative effect of a plaintiff's decision to stand on its complaint. [*See* Paytime's November 20, 2015 submission at 6].

Here, Employees' election to stand on their proposed CAC similarly forecloses the possibility of further litigation on the merits.[4] Employees do not intend to make another attempt to cure the supposed deficiencies the District Court identified in their proposed CAC. Instead, they stood on the CAC's allegations and are arguing to this Court that those allegations were sufficient to establish

[4] Employees were not required to file a formal statement with the District Court electing to stand on their proposed CAC to make final the Order of October 6, 2015. The mere filing of the Joint Notice of Appeal is enough to make the Order of October 6 final. *See e.g.*, *Frederico v. Home Depot*, 507 F.3d 188, 192 (3d Cir. 2007) (holding that dismissal of complaint without prejudice was a final order where the plaintiff's "only response was to file a notice of appeal"). Moreover, although Employees intended to stand on their proposed CAC when they filed their notice of appeal, their explicit statement of intent in their November 20 submission is sufficient to make the Order of October 6 a final order. *See e.g.*, *Tiernan v. Devoe*, 923 F.2d 1024, 1031 (3d Cir. 1991) (holding that the district court's summary enforcement of settlement agreements between plaintiffs and three out of four groups of defendants, although not appealable at the time the appeal was filed, was appealable later because the plaintiffs/appellants renounced any intention to take further action against the fourth group of defendants through letter briefs to the Third Circuit).

Employees' standing. As a result, once Employees filed their notice of appeal, the District Court's Order of October 6, 2015 became final.

Requiring Employees to return to the District Court and declare their intent to stand on their proposed CAC, and obtain an explicit dismissal with prejudice and a separate judgment "would be a wasteful elevation of form over substance," *Shapiro*, 964 F.2d at 278, and also would fail to serve any practical purpose:

> If, by error, a separate judgment is not filed before a party appeals, nothing but delay would flow from requiring the court of appeals to dismiss the appeal. Upon dismissal, the district court would simply file and enter the separate judgment, from which a timely appeal would then be taken. Wheels would spin for no practical purpose.

Id. at 279 (quoting *Bankers Trust Co. v. Mallis*, 435 U.S. 381, 385 (1978)). As such, the Order of October 6, 2015 should be treated as a final order of dismissal given the present circumstances.

Accordingly, the October 6, 2015, Memorandum and Order finding the proposed CAC futile and denying Employees' motion for leave is final and appealable under this Court's interpretation of 28 U.S.C. § 1291.

ii. The Order of March 13, 2015 Was Not Final Within the Meaning of 28 U.S.C. § 1291

The Order dated March 13, 2015, was not an appealable final order. "[A]n order dismissing a complaint without prejudice is ordinarily not appealable," unless "the plaintiff…elects to stand on the complaint without amendment…."

Bethel, 81 F.3d at 381. Here, Employees *did not* elect to stand on the *Storm* Amended Complaint or the *Holt* Complaint. Instead, all Plaintiffs-Appellants filed a Motion for Leave to File the proposed CAC, which they believed adequately alleged the facts giving rise to their standing. Therefore, the initial March 13, 2015 dismissal was not an appealable final order. *See Cycle Chem, Inc. v. Jackson*, 465 Fed. Appx. 104, 107 (3d Cir. 2012) (finding that a September 4, 2008, order of dismissal and denial, without prejudice, of a motion for leave to file a second amended complaint was not a final order because the plaintiff "did not elect to stand on the complaint without amendment; instead, [the plaintiff] renewed its motion to file a second amended complaint, which it believed alleged wrongdoing that did not form the basis of the complaint that the District Court dismissed"). As a result, Employees properly appealed the Order of October 6, 2015, which was appealable for the reasons stated above.

iii. Appellate Jurisdiction is Proper Because Employees Filed a Timely Notice of Appeal

This Court has jurisdiction over the appeal of the final October 6, 2015 Order. A party may take an appeal as of right if she files a notice of appeal "with the district clerk within 30 days after entry of judgment or order appealed from." Fed. R. App. P. 4(a)(1). Here, Appellants-Employees filed their Joint Notice of Appeal 28 days after the District Court's final Order of October 6. Accordingly, this Court has jurisdiction over the appeal of the Order of October 6.

This Court also has jurisdiction over the appeal of the District Court's Order of March 13, 2015. It is well-established that "prior interlocutory orders…merge with the final judgment in a case, and the interlocutory orders (to the extent that they affect the final judgment) may be reviewed on appeal from the final order." *Camesi v. U. of Pittsburgh Med. Ctr.*, 729 F.3d 239, 244-45 (3d Cir. 2013). As a result, the Order of March 13 merged with the Order of October 6. Therefore, this Court has jurisdiction over the appeal of the Order of March 13 as well.

For the forgoing reasons, the October 6, 2015, Order was final and appealable, and this Court has jurisdiction over Employees' appeal.

VIII. CONCLUSION

For the forgoing reasons, the Employees-Appellants respectfully request that this Court reverse the March 13, 2015, and October 6, 2015, Orders of the District Court, and remand this case to the district court for further proceedings.

Dated: April 11, 2016

Respectfully submitted,

By: /s/ Gary F. Lynch

CARLSON LYNCH SWEET & KILPELA LLP
Gary F. Lynch
Edwin J. Kilpela
Jamisen A. Etzel
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
(p) (412) 322-9243
(f) (412) 231-0246

LITE DEPALMA GREENBERG LLC
Katrina Carroll
211 West Wacker Drive, Suite 500
Chicago, IL 60606
(p) (312) 750-1265

LITE DEPALMA GREENBERG LLC
Mindee J. Reuben
1521 Locust Street, 7th Floor
Philadelphia, PA 19102
(p) (267) 519 8306
(f) (215) 569-0958

LOCKRIDGE GRINDAL NAUNEN PLLP
Karen H. Riebel
Eric N. Linsk
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
(p) (612) 339-6900

MEREDITH & NARINE
Joel C. Meredith
Krishna B. Narine
100 South Broad Street, Suite 905
Philadelphia, PA 19110
(p) (215) 564-5182
(f) (215) 569-0958

Attorneys for Appellants

COMBINED CERTIFICATIONS

I, Gary F. Lynch, signing counsel for Appellants, hereby certify as follows:

1. Pursuant to Rule 46.1 of the Local Appellate Rules for the United States Court of Appeals for the Third Circuit, I certify that I am a member in good standing of the bar of the United States Court of Appeals for the Third Circuit.

2. Pursuant to Federal Rule of Appellate Procedure 32(a)(7)(c), I certify that this Brief of Appellants complies with the type and volume limitations of Fed. R. App. P. 32(a)(7)(B):

   a. According to the word count in the word processing system employed in drafting this brief (Microsoft Word 2013), the Brief of Appellee contains 9,274 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

   b. This Brief has been written in Times New Roman, a proportionally-spaced, 14-point serif font.

3. On today's date, April 11, 2016, I filed this brief with the Clerk of the United States Court of Appeals for the Third Circuit via the Court's CM/ECF system, which will cause service on counsel for all parties of record, who are registered CM/ECF Users.

4. I further certify that the E-Brief was scanned for computer viruses using the current version of VirusTotal scanning service, and no virus was detected.

5. I also certify that the text of the hard copies and the E-Brief are identical.

/s/ Gary F. Lynch
Gary F. Lynch (PA#56887)
CARLSON LYNCH SWEET & KILPELA LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
(p) (412) 322-9243
(f) (412) 231-0246
glynch@carlsonlynch.com

Attorney for Appellants

CASE NO. 15-3690

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

DANIEL B. STORM, *et al.*,
Appellants

v.

PAYTIME, INC.,
Appellee.

Appeal from the Orders of the United States District Court For the Middle District of Pennsylvania in Civil Action Nos. 14-1138 and 14-3964 (Jones, J.)

JOINT APPENDIX – VOLUME I of II (JA0001-JA0034)

CARLSON LYNCH SWEET & KILPELA LLP
Gary F. Lynch
Edwin J. Kilpela
Jamisen A. Etzel
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
(p) (412) 322-9243
(f) (412) 231-0246

Additional Attorneys
Listed on Inside Page

Attorneys for Appellants

April 11, 2016

LITE DEPALMA GREENBERG LLC
Katrina Carroll
211 West Wacker Drive, Suite 500
Chicago, IL 60606
(p) (312) 750-1265

LITE DEPALMA GREENBERG LLC
Mindee J. Reuben
1521 Locust Street, 7th Floor
Philadelphia, PA 19102
(p) (267) 519 8306
(f) (215) 569-0958

LOCKRIDGE GRINDAL NAUNEN PLLP
Karen H. Riebel
Eric N. Linsk
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
(p) (612) 339-6900

MEREDITH & NARINE
Joel C. Meredith
Krishna B. Narine
100 South Broad Street, Suite 905
Philadelphia, PA 19110
(p) (215) 564-5182
(f) (215) 569-0958

Attorneys for Appellants

TABLE OF CONTENTS

Volume I: *Page*

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

DANIEL B. STORM, HOLLY P. WHITE, DORIS MCMICHAEL, and KYLE WILKINSON, individually and on behalf of all others similarly situated Plaintiffs, v. PAYTIME, INC., Defendant.	:	Case No.: 1:14-cv-1138-JEJ Hon. John E. Jones III
BARBARA HOLT AND LINDA REDDING, individually and on behalf of all others similarly situated, Plaintiffs, v. PAYTIME HARRISBURG, INC., d/b/a PAYTIME, INC., a Pennsylvania corporation, Defendant.	:	

JOINT NOTICE OF APPEAL

Notice is hereby given that in accordance with Federal Rules of Appellate Procedure 3 and 4, and 28 U.S.C. § 1291, Plaintiffs Barbara Holt, Doris McMichael, Linda Redding, Daniel B. Storm, Holly P. White and Kyle Wilkinson ("Plaintiffs") in the above-captioned consolidated matter, appeal to the United States Court of

Appeals for the Third Circuit from the Order of the Honorable John E. Jones, III, entered on October 06, 2015, [Dkt. No. 53] denying Plaintiffs' Motion for Leave to File First Consolidated Amended Class Action Complaint, and the Order and Memorandum entered March 13, 2015 [Dkt. Nos. 48, 49] granting Defendants' Motion to Dismiss the First Amended Complaint in *Storm et al. v. Paytime, Inc.*, No. 14-cv-1138 (M.D. Pa.), and the Complaint in *Holt et al. v. Paytime Harrisburg, Inc.*, No. 1:14-cv-01968 (M.D. Pa.) (originally No. 14-cv-3964 (E.D. Pa.)). Plaintiffs respectfully request that all documents filed in this case (and in No. 1:14-cv-01968) be transmitted with the record on appeal.

Dated: November 3, 2015

Respectfully submitted,

By: /s/ *Gary F. Lynch*

Gary F. Lynch
glynch@carlsonlynch.com
Edwin J. Kilpela, Jr.
ekilpela@carlsonlynch.con
Jamisen A. Etzel
jetzel@carlsonlynch.com
Carlson Lynch Sweet & Kilpela, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Phone: (412) 322-9243
Fax: (412) 231-0246

Michael L. Kraemer
m@lawkm.com
David M. Manes
david@lawkm.com
Elizabeth Pollock-Avery
elizabeth@lawkm.com
Kraemer, Manes & Associates LLC
US Steel Tower
600 Grant Street, Suite 660
Pittsburgh, PA 15219
Phone: (412) 626-5626
Fax: (412) 637 0232

Joel Meredith
jmeredith@m-npartners.com
Meredith & Narine
100 Broad St.
Suite 905
Philadelphia, PA 19110
Phone: (215) 564-5182
Fax: (215) 569-0958

Steven Greenfogel
sgreenfogel@litedepalma.com
Lite DePalma Greenberg, LLC
1521 Locust Street – 7th Floor
Philadelphia PA 19102
Phone: (267) 519 8306
Fax: (215) 569 0958

Katrina Carroll
kcarroll@litedepalma.com
Kyle A. Shamberg
kshamberg@litedepalma.com
Lite DePalma Greenberg, LLC
Chicago Office
211 West Wacker Drive
Suite 500
Chicago, IL 60606
Phone: (312) 750 1265

Karen H. Riebel
khriebel@locklaw.com
Eric N. Linsk
rnlinsk@locklaw.com
Lockridge Grindal Nauen PLLP
100 Washington Avenue South,
Suite 2200
Minneapolis, MN 55401
Phone: (612) 339-6900

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I, Gary F. Lynch, hereby certify that a true and correct copy of the foregoing Notice of Appeal was filed with the Clerk of Court using the CM/ECF system, which will serve all counsel of record via a notification of electronic filing (NEF) on this 3rd day of November, 2015.

/s/ *Gary F. Lynch*
Gary F. Lynch

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

DANIEL B. STORM, HOLLY P. WHITE, DORIS MCMICHAEL, and KYLE WILKINSON, individually and on behalf of all others similarly situated, Plaintiffs,	:	14-cv-1138
v.	:	
PAYTIME, INC., Defendant.	:	
_____	:	Hon. John E. Jones III
BARBARA HOLT and LINDA REDDING, individually and on behalf of all others similarly situated, Plaintiffs,	:	
v.	:	
PAYTIME HARRISBURG, INC., d/b/a PAYTIME, INC., a Pennsylvania corporation, Defendant.	:	

ORDER

March 13, 2015

In accordance with the Memorandum issued on today's date, it is hereby

ORDERED that:

1. Defendant's Motions to Dismiss the Amended Complaint (Doc. 28) in

Storm and the Complaint in *Holt* are **GRANTED**.

2. The First Amended Class Action Complaint (Doc. 17) in *Storm* and the Complaint in *Holt* (Doc. 1) are **DISMISSED WITHOUT PREJUDICE**, in their entirety.

3. The Clerk of Court is directed to **CLOSE** the consolidated case.

s/ John E. Jones III
John E. Jones III
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

DANIEL B. STORM, HOLLY P. WHITE, DORIS MCMICHAEL, and KYLE WILKINSON, individually and on behalf of all others similarly situated, Plaintiffs,	:	14-cv-1138
v.	:	
PAYTIME, INC., Defendant.	:	
	:	Hon. John E. Jones III
BARBARA HOLT and LINDA REDDING, individually and on behalf of all others similarly situated, Plaintiffs,	:	
v.	:	
PAYTIME HARRISBURG, INC., d/b/a PAYTIME, INC., a Pennsylvania corporation, Defendant.	:	

MEMORANDUM

March 13, 2015

There are only two types of companies left in the United States, according to data security experts: "those that have been hacked and those that don't know

they've been hacked."[1] According to a 2014 report conducted by the Ponemon Institute, 43% of companies have experienced a data breach in the past year. Even worse, the absolute size of the breaches is increasing exponentially.[2] When our fellow citizens hear statistics such as these, they are understandably worried about the privacy of their most personal information, such as their Social Security numbers and bank account information. Further, when a data breach occurs, especially one intentionally done by a hacker, it is not unreasonable for the victims to feel that a wrong has clearly been committed. But has there been an actionable harm that is cognizable in federal court? This is the question with which we must grapple in the matter *sub judice*.

Pending before the Court are two putative class actions concerning a security breach of Defendant Paytime, Inc.'s ("Paytime") computer systems, in which an unknown third party allegedly accessed Plaintiffs' confidential personal and financial information. These cases have been consolidated. Prior to consolidation, Paytime filed in each case a Motion to Dismiss Pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), contending that Plaintiffs lack standing, or in the

---

[1] Nicole Perlroth, *The Year in Hacking, by the Numbers*, N.Y. TIMES, Apr. 22, 2013, http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/?_r=0.

[2] Elizabeth Weise, *43% of Companies Had a Data Breach in the Past Year*, USA TODAY, Sept. 24, 2014, http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/.

alternative, that they have failed to state claims as a matter of law. Paytime also filed a Motion to Strike Class Allegations Pursuant to Federal Rule of Civil Procedure 12(f) in each case. For the reasons that follow, we will dismiss the consolidated case for lack of standing, and accordingly, not address Paytime's other motions.

I. PROCEDURAL HISTORY

On February 18, 2015, *Storm, et al. v. Paytime, Inc.* and *Holt, et al. v. Paytime, Inc.* were consolidated into one case for the remainder of the proceedings between the parties. (*Storm*, Doc. 46). However, due to the fact that these cases were filed separately and have had filings and motions pending in separate dockets, we will discuss their procedural histories separately.

In *Storm*, on June 13, 2014, Plaintiffs filed a Complaint against Paytime, alleging claims of negligence and breach of contract. (*Id.*, Doc. 1). The Complaint also included class action allegations under Federal Rule of Civil Procedure 23. Plaintiffs allege that as many as 233,000 individuals could be members of the class, as that is approximately how many individuals who had their personal and financial information allegedly compromised.

By agreement of the parties, Paytime's response to the Complaint was due August 1, 2014. (*Id.*, Doc. 7). On that date, Paytime filed a motion to dismiss for

failure to state a claim upon which relief may be granted and for lack of standing. (*Id.*, Doc. 12). In response to this motion, Plaintiffs filed an Amended Complaint on August 8, 2014. (*Id.*, Doc. 17). Again by agreement of the parties, Paytime's response to the Amended Complaint was due August 27, 2014. (*Id.*, Doc. 18).

On August 27, 2014, Paytime filed the instant Motion to Dismiss for failure to state a claim and for lack of jurisdiction. (*Id.*, Doc. 28). On the same date, Paytime filed its brief in support of the Motion. (*Id.*, Doc. 29). After being granted an extension of time to file its response, Plaintiffs filed their brief in opposition to the Motion on September 24, 2014. (*Id.*, Doc. 37). Paytime filed a reply brief on October 7, 2014. (*Id.*, Doc. 41). Thus, having been fully briefed, this Motion is now ripe for our review.[3]

Turning to the procedural history of *Holt et al. v. Paytime*, Plaintiffs in that case originally filed their putative class action lawsuit against Paytime in the United States District Court for the Eastern District of Pennsylvania on June 27,

[3] In addition to the Motions to Dismiss, Paytime also filed Motions for Leave to File a Third Party Complaint. (*Storm*, Doc. 38; *Holt*, Doc. 31). Paytime seeks to join Netcomm Solutions, Inc., d/b/a SotirIS Information Strategies ("SotirIS") as a Third Party Defendant. Paytime filed briefs in support of these Motions. (*Storm*, Doc. 39, *Holt*, Doc. 32). However, Plaintiffs never filed briefs in opposition to these Motions, and their time do so has long expired. Pursuant to Local Rule 7.6, the Motions are deemed unopposed. While we ordinarily would grant an unopposed motion, because we will be granting the Motions to Dismiss in their entirety, the Motions for Leave to File a Third Party Complaint are now moot and should be dismissed as such.

2014. (*Holt*, Doc. 1). In their Complaint, they alleged causes of action under breach of contract and Pennsylvania's Unfair Trade Practices and Consumer Protection Law (UTPCPL). On August 4, 2014, Paytime filed a Motion to Dismiss Pursuant to Federal Rules of Civil Procedure 12(b)(1) & 12(b)(6). (*Id.*, Doc. 5). A day later, on August 5, 2014, Paytime filed a Motion to Transfer Venue to the Middle District of Pennsylvania. (*Id.*, Doc. 6). On September 3, 2014, Plaintiffs filed their brief in opposition to the Motion to Dismiss. (*Id.*, Doc. 12). Paytime filed its reply brief on September 11, 2014. (*Id.*, Doc. 18).

By court order, on September 26, 2014, *Holt* was transferred to the Middle District of Pennsylvania. (*Id.*, Doc. 21). The matter was filed in this Court on October 10, 2014. (*Id.*, Doc. 22).

Because the Motion to Dismiss pending in *Holt* has been fully briefed, this matter is also ripe for our review, as part of the consolidated case.

II. STANDARD OF REVIEW

Because we need only address Paytime's jurisdictional arguments, Federal Rule of Civil Procedure 12(b)(1) provides the relevant legal standard.

A court must grant a motion to dismiss if it determines it lacks subject matter jurisdiction to hear a case. *See* FED. R. CIV. P. 12(h)(3). A motion to dismiss based on a lack of standing is a jurisdictional matter and thus "properly brought pursuant

to Rule 12(b)(1)." *Ballentine v. United States*, 486 F.3d 806, 810 (3d Cir. 2007). When considering a motion to dismiss under Rule 12(b)(1), a court must distinguish between facial and factual challenges to its subject matter jurisdiction. *See Mortensen v. First Fed. Sav. & Loan Ass'n*, 549 F.2d 884, 891 (3d Cir. 1977). A facial attack challenges whether the plaintiff has properly pled jurisdiction. *Id.* "In reviewing a facial attack, the court must only consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff." *Gould Elecs., Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000) (citing *Mortensen*, 549 F.2d at 891). A factual attack, in contrast, challenges jurisdiction based on facts apart from the pleadings. *Mortensen*, 549 F.2d at 891. "When a defendant attacks subject matter jurisdiction 'in fact,' . . . the Court is free to weigh the evidence and satisfy itself whether it has power to hear the case. In such a situation, 'no presumptive truthfulness attaches to plaintiff's allegations, and the existence of disputed material facts will not preclude the trial court from evaluating for itself the merits of jurisdictional claims.'" *Carpet Group Int'l v. Oriental Rug Importers Ass'n*, 227 F.3d 62, 69 (3d Cir. 2000) (quoting *Mortensen*, 549 F.2d at 891).

Here, Paytime asserts a facial challenge to this Court's subject matter jurisdiction to hear the instant case.

III. FACTUAL SUMMARY

In accordance with the standard of review applicable to a Rule 12(b)(1) Motion to Dismiss, the following facts are derived from the complaints underlying the consolidated case and are viewed in the light most favorable to the Plaintiffs.

As the parties are aware, we issued an order consolidating these matters. In large part, the factual underpinnings are identical; however, where there are distinctions, we will identify those distinctions.

Paytime is a national payroll service company that offers a variety of services to its clients, including human resource management services, time and attendance systems, and web-based payroll submission. (*Storm*, Doc. 17, ¶ 6). Plaintiffs and putative class members are current or former employees of companies that used Paytime as their payroll processing service. (*Id.*, ¶¶ 8-11).

In order to facilitate payroll processing, Plaintiffs and the proposed class members were required to provide to their employers confidential personal and financial information, including their full legal names, addresses, bank account data, Social Security numbers, and dates of birth. (*Id.*, ¶ 14). This sensitive information was then provided to Paytime. (*Id.*, ¶ 15).

On April 7, 2014, unknown third parties gained unauthorized access to Paytime's computer systems. Paytime did not discover this security breach until

April 30, 2014. (*Id.*, ¶ 17). Plaintiffs further allege that Paytime waited until May 12, 2014 to begin to notify affected parties that there had been a security breach. (*Id.*, ¶ 18). On May 20, 2014, Paytime disclosed that forensic experts had conducted an investigation into the breach, and were able to confirm that the data breach had in fact occurred, and that the confidential personal information of employees of their clients had been accessed by these unknown third parties. (*Id.*, ¶ 19). Plaintiffs allege that nationally, over 233,000 individuals had their personal and financial information "misappropriated" as a result of the breach of Paytime's computer network. (*Id.*, ¶ 20).

Plaintiffs allege that as a result of this data breach, they and the proposed class members have spent, or will need to spend, time and money to protect themselves from identity theft. (*Id.*, ¶ 28). Plaintiffs assert they have suffered actual damages, as well. As an "example" of these damages, Plaintiffs point to Plaintiff Wilkinson, who is an employee of a government contractor and must have security clearances in order to perform his job. After Paytime's data breach, Wilkinson reported the incident to this employer, who then suspended his security clearances while the employer investigated the situation. (*Id.*, ¶ 29). During the investigation, Wilkinson was required to work at a different job site, resulting in a four hour increase in his daily commute. This increased commute caused Wilkinson to incur

travel expenses in addition to lost time. (*Id.*).

Plaintiffs in *Holt* allege similar injuries and actual damages, such as costs of monitoring their financial accounts, the opportunity cost of the time spent monitoring their accounts for identity theft, and costs of obtaining replacement checks and/or credit and debit cards. (*Holt*, Doc. 1, ¶ 40). They also allege as injuries "the significant possibility of monetary losses arising from unauthorized bank account withdrawals, fraudulent payments, and/or related bank fees charged to their accounts." (*Id.*, ¶ 36). As in *Storm*, they also allege as an injury the increased risk of identity theft. (*Id.*, ¶ 39).

Paytime has offered to provide free credit monitoring and identity restoration services for twelve (12) months for all persons affected by the data breach. (*Storm*, Doc. 37, Ex. B).

IV. DISCUSSION

First, we will consider whether Plaintiffs have standing to bring this case, based on the factual allegations of their Complaints. If none have standing, of course, we must dismiss the matter *sub judice*. If any Plaintiffs do have standing, we will then consider whether they have stated a claim for which relief can be granted.

Article III courts are courts of limited jurisdiction. As a constitutional

matter, federal courts only have jurisdiction over actual "cases or controversies." U.S. CONST. art. III, § 2. One element of this limitation is that plaintiffs have the burden of establishing they have standing to sue. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Standing analysis focuses on whether the "plaintiff is the proper party to bring this suit." *Raines v. Byrd*, 521 U.S. 811, 818 (1997) (citing *Simon v. Eastern Ky. Welfare Rights Organization*, 426 U.S. 26, 38 (1976)). More specifically, the classical formulation of standing requirements is that "a plaintiff must allege personal injury fairly traceable to the defendant's allegedly unlawful conduct and likely to be redressed by the requested relief." *Allen v. Wright*, 468 U.S. 737, 751 (1984). Procedurally, this translates to a requirement that a plaintiff must allege sufficient factual allegations in his or her complaint in order to establish standing. *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990).

The personal injury element of standing requires an "injury in fact"–one that is "concrete in both a qualitative and temporal sense," as opposed to merely "abstract." *Id.* The injury must also be actual or "imminent," not "conjectural" or "hypothetical." *Id.* (internal citations omitted). The imminency requirement has caused some consternation among the courts, leading the United States Supreme Court to expound on what an "imminent" injury entails in order to clarify this somewhat abstract concept. "Allegations of possible future injury do not satisfy the

requirements of Art. III. A threatened injury must be 'certainly impending' to constitute injury in fact." *Id.* at 158 (citing to a long history of Supreme Court cases standing for this proposition). Recently, in *Clapper v. Amnesty Intern. USA*, 133 S.Ct. 1138 (2013), the Supreme Court reiterated that a threatened injury must be "certainly impending." *Id.* at 1147.[4] This standard establishes a high bar for plaintiffs seeking to recover for injuries which have not in fact occurred, even if they appear likely or probable. With this rigorous standard, courts seek to "reduce the possibility of deciding a case in which no injury would have occurred at all." *Lujan*, 504 U.S. at 564 n.2.

The Third Circuit has provided guidance on standing and its imminency requirement for future injuries, specifically in the context of data breaches, as these have unfortunately become common occurrences in the modern world. The Third Circuit has held that in the event of a data breach, a plaintiff does not suffer a

[4] Plaintiffs correctly point out that the Supreme Court in *Clapper* included a footnote in their opinion which states that "in some instances," a "substantial risk" that the harm will occur would be sufficient to confer standing on a plaintiff. *Id.* at 1150 n.5. This teasing footnote does indeed invite confusion in standing jurisprudence. However, in the case before us, we choose to rely on the standard the Court relied on for its holding in *Clapper*, rather than a footnote. Furthermore, *Reilly,* discussed *infra*, provides us with precedential guidance on standing specifically in the context of data breach cases. And as point of fact, if we were to apply the "substantial risk" standard, Plaintiffs have not met that bar, either. They allege that an identity fraud research study found that "nearly 1 in 4 data breach letter recipients became a victim of identity fraud . . . ." (*Storm*, Doc. 17, ¶ 23). A 25 % chance of Plaintiffs becoming identity fraud victims is not a substantial risk. By Plaintiffs' own calculations, injury is not impending for 75% of victims of the Paytime breach. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, No. 12-347, 2014 WL 1858458, *7 (D. D.C. May 9, 2014).

harm, and thus does not have standing to sue, unless plaintiff alleges actual "misuse" of the information, or that such misuse is imminent. *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011). In *Reilly*, employees of a law firm brought a putative class action against a payroll processing firm, called Ceridian, after Ceridian suffered a security breach by an unknown hacker. *Id.* at 40. There, the plaintiffs harbored concerns about the breach because Ceridian had their personal and financial information stored as data, including the names of the plaintiffs, their Social Security numbers, and in some cases, their birth dates and bank account information. *Id.* Plaintiffs sued Ceridian under negligence and breach of contract theories of liability, alleging that due to the data breach, they were subject to an increased risk of identity theft, had incurred costs to monitor their credit activity, and suffered from emotional distress. *Id.*

The Third Circuit affirmed the district court's dismissal of the case, on the ground that the plaintiffs lacked Article III standing. *Id.* at 41. The circuit court reasoned that plaintiffs' alleged future harm resulting from the security breach was not sufficiently imminent to meet the threshold for standing–the risk of future injury was significantly attenuated, considering that it was "dependent on entirely speculative, future actions of an unknown third party." *Id.* at 42. The court pointedly elaborated:

> "We cannot now describe how Appellants will be injured in this case without beginning our explanation with the word 'if': *if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will Appellants have suffered an injury." *Id.* at 43 (emphasis in original).

Thus, the Third Circuit requires its district courts to dismiss data breach cases for lack of standing unless plaintiffs allege actual misuse of the hacked data or specifically allege how such misuse is certainly impending. Allegations of increased risk of identity theft are insufficient to allege a harm. *Id.* at 43.

Turning again to the matter *sub judice*, we will review Plaintiffs' factual allegations from the Amended Complaint in the consolidated case, and any distinctive allegations from the Complaint in *Holt*, to decide whether they allege an injury that is either actual or imminent. Here, the factual allegations are remarkably similar to those of *Reilly*. Plaintiffs allege that their personal and financial data were "obtained" "by unknown third parties." (*Storm*, Doc. 17, ¶ 2). They allege that this information was "accessed without their authorization" and "misappropriated." (*Id.*, ¶¶ 16, 20). Plaintiffs allege that as a result of the data breach, they and the proposed class members "are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse." (*Id.*, ¶ 27). Additionally, they have spent, or foresee spending, time and money to protect themselves from identity theft. (*Id.*, ¶ 28). They also allege that some Plaintiffs and

proposed Class Members have suffered actual damages as a result of the data breach. They specifically cite one person, Plaintiff Wilkinson, who is employed by a government contractor. (*Id.*, ¶ 29). Wilkinson's job requires him to have security clearances. Plaintiffs allege that after reporting the data breach to his employer, Wilkinson's "security clearances had to be suspended for a period of time so that his employer could investigate the situation." Due to this situation, Wilkinson was required to work at a different job site than his usual one and his commute time was significantly increased, resulting in loss of time and travel expenses. (*Id.*).

Reviewing these allegations, the Court finds no factual allegation of misuse or that such misuse is certainly impending. Plaintiffs do not allege that they have actually suffered any form of identity theft as a result of the data breach–to wit, they have not alleged that their bank accounts have been accessed, that credit cards have been opened in their names, or that unknown third parties have used their Social Security numbers to impersonate them and gain access to their accounts. *See Reilly*, 664 F.3d at 45. In sum, their credit information and bank accounts look the same today as they did prior to Paytime's data breach in April 2014. Under *Reilly*, we find that Plaintiffs have not alleged an actual injury.

Plaintiffs argue that the different verbs used in their allegations, such as "stolen" and "misappropriated," distinguish their case from *Reilly* in such a way as

to create a cognizable harm, but this is a strained argument, which would require the Court to ignore the substance of the allegations. In the complaint at issue in *Reilly*, plaintiffs alleged that an "outside hacker" was able to "infiltrate" the defendant's security system and "gain access" to confidential and personal information of the plaintiffs. Complaint at ¶ 11, *Reilly v. Ceridian Corp.*, 2011 WL 735512 (D. N.J. Feb. 22, 2011) (No. 10-5142). In the matter *sub judice*, Plaintiffs somewhat artfully chose other verbs, but to draw a distinction of substance would require us to elevate the thesaurus above our logic and common sense. At the core of both cases, plaintiffs alleged a hacker broke into the defendant's data system and accessed it to some degree. Implicit in the *Reilly* complaint, of course, is that the access was without permission–thus, they also effectively alleged that the data was "misappropriated," as was alleged in the instant case. However, regardless of verbiage, Plaintiffs have only alleged the data was accessed by an unknown third party. There is no allegation that the hacker caused a new bank account or credit card to be opened in any of Plaintiffs' names, or any other form of identity theft. In other words, Plaintiffs have not alleged actual "misuse" of the data, which is the touchstone of the *Reilly* standard. *Reilly* draws a clear line in the sand in this context as to when a data breach becomes a harm. While some may argue that the line should be more favorable to plaintiffs and could perhaps be drawn at the

moment the data is accessed, that is not the extant standard.

Further, Plaintiffs' alleged harm–that they are now at an increased risk of identity theft–does not suffice to allege an imminent injury. *Reilly*, 664 F.3d at 43.[5] Perhaps this strict imminency standard has some wisdom, for even though Plaintiffs may indeed be at greater risk of identity theft, the data breach in this case occurred in April 2014–almost a year ago– and Plaintiffs have yet to allege that any of them have become actual victims of identity theft. Indeed, putting aside the legal standard for imminence, a layperson with a common sense notion of "imminence" would find this lapse of time, without any identity theft, to undermine the notion that identity theft would happen in the near future. [6]

Plaintiffs cite *Reilly*'s discussion of the facts of *Pisciotta v. Old National Bancorp.*, 499 F.3d 629 (7th Cir. 2007), and how they are distinguishable from those of *Reilly* itself, to argue that the harm in the instant case is more "imminent" by virtue of the fact the breach was done by skilled hackers working from

---

[5] "Appellants' allegations of an increased risk of identity theft resulting from a security breach are therefore insufficient to secure standing." *Reilly*, 664 F.3d at 43 (citing to *Whitmore*, 495 U.S. at 158).

[6] The logic of this paragraph also applies to the allegation in *Holt* that one of Plaintiffs' injuries in fact or actual damages is "the significant possibility of monetary losses arising from unauthorized bank account withdrawals, fraudulent payments, and/or related bank fees charged to their accounts." (*Holt*, Doc. 1, ¶ 36). This is effectively just a more detailed form of alleging that Plaintiffs are at an increased risk of identity theft. Further, a "possibility" of monetary losses resulting from a data breach does not state a harm.

"foreign" IP addresses. First, even if the hackers here were more skilled or "malicious," although this seems to be quite a speculative assessment for a party or court to make, the fact remains that the harm of misuse has yet to occur, almost a year later, which undercuts the imminency argument. Further, we note that *Pisciotta* did not mention the imminency requirement for threatened injuries for constitutional standing purposes, so we do not find that court's reasoning particularly persuasive on this issue. *Reilly*, 664 F.3d at 44.

Based on the failure to allege facts showing a misuse of data or that such misuse is imminent, *Clapper* and *Reilly* direct us to dismiss Plaintiffs for lack of standing without too much hesitation. This disposition is in line with the vast majority of courts who have reviewed data breach cases where no misuse was alleged post-*Clapper*. *See, e.g., In re SAIC*, 2014 WL 1858458, at *8 ("This is not to say that courts have uniformly denied standing in data-breach cases. Most cases that found standing in similar circumstances, however, were decided pre-*Clapper* or rely on pre-*Clapper* precedent and are, at best, thinly reasoned.") (citations omitted); *Strautins v. Trustwave Holdings, Inc.*, 27 F.Supp.3d 871 (N.D.Ill. 2014); *Polanco v. Omnicell, Inc.*, 988 F.Supp.2d 451 (D.N.J. 2013).

However, Plaintiffs point to one of themselves, Kyle Wilkinson, as someone who has suffered actual damages, or actual injury, due to the data breach,

ostensibly to create a foothold in our jurisdiction. His supposed damages, in the form of increased commute time and related expenses, although surely unfortunate, are merely a form of prophylactic costs the Supreme Court has warned cannot be used to "manufacture" standing, even if those costs are reasonable. *Clapper*, 133 S.Ct. at 1151. In *Clapper*, the Court reasoned, "Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending." *Id.* Wilkinson's preventive measure taken–working from a different job site while his security clearance was reviewed– is different in form but not in substance from the classic forms of preventive measures taken in data breach cases, such as credit monitoring. Based on the applicable precedent, there is still no misuse of his data, and thus no injury.

Although this stringent standard for standing does leave Wilkinson and the other Plaintiffs to foot the bill for their preventive measures taken[7], the logic of the doctrine is sound, and the application of it in the context of the recent rash of data breach cases makes its wisdom all the more clear. Hackers are constantly seeking to gain access to the data banks of companies around the world. Sometimes, they

[7] However, Paytime has arranged to provide free credit monitoring for 12 months for all persons affected by the data breach, so Plaintiffs will not in fact have to pay for many of their reasonable preventive costs. (Doc. 37, Ex. B).

are successful. Other times not. Despite many companies' best efforts and tremendous expense to secure and protect their data systems, an industrious hacker every so often may find a way to access their data. Millions of people, out of reasonable fear and prudence, may decide to incur credit monitoring costs and take other preventive steps, which the hacked companies often freely provide.[8] However, for a court to require companies to pay damages to thousands of customers, when there is yet to be a single case of identity theft proven, strikes us as overzealous and unduly burdensome to businesses. There is simply no compensable injury yet, and courts cannot be in the business of prognosticating whether a particular hacker was sophisticated or malicious enough to both be able to successfully read and manipulate the data and engage in identity theft. Once a hacker does misuse a person's personal information for personal gain, however, there is a clear injury and one that can be fully compensated with money damages. *See Reilly*, 664 F.3d at 45-46. In that situation, a plaintiff would be free to return to court and would have standing to recover his or her losses.

---

[8] Hayley Tsukayama, *Target says customers signing up for free credit monitoring after data breach*, WASH. POST, Jan. 13, 2014, http://www.washingtonpost.com/business/technology/target-says-customers-signing-up-for-free-credit-monitoring-after-data-breach/2014/01/13/99fcce60-7c83-11e3-95c6-0a7aa80874bc_story.html; Tara Siegel Bernard, *What Anthem Customers Should Do Next After the Data Breach*, N.Y.TIMES, Feb. 6, 2015, http://www.nytimes.com/2015/02/07/your-money/what-anthem-customers-should-do-next-after-data-breach.html.

Plaintiffs also contend that they have alleged actual injury based on harm to their privacy interest, in having their confidential personal information accessed by an unauthorized third party. "For a person's privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party . . . if no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated." *In re SAIC Litig.*, 2014 WL 1858458, at * 19 (citing 5 C.F.R. § 297.102). Here, Plaintiffs do not allege that the unidentified hacker was actually able to view, read, or otherwise understand the data it accessed. They do not allege that their information was exposed in such a way as to make it easily viewed. *Reilly* addressed this issue as well, noting that it is speculative that the hacker "read, copied, or understood the data." 664 F.3d at 40. Consequently, Plaintiffs have not alleged that harm to their privacy interest is actual or imminent.

Because we conclude that Plaintiffs lack standing and thus must dismiss the case, we need not address Paytime's other arguments for dismissal made in their Motion.

V. CONCLUSION

In conclusion, Plaintiffs have failed to plead specific facts demonstrating they have standing to bring this suit under Article III. Consistent with our above

discussion, we will grant Paytime's motion to dismiss, as set forth more fully hereinabove and as follows. Because we are dismissing the instant case for lack of standing under Rule 12(b)(1), the dismissal is without prejudice.

A separate Order consistent with this Memorandum shall follow.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

DANIEL B. STORM, HOLLY P. WHITE, DORIS MCMICHAEL, and KYLE WILKINSON, individually and on behalf of all others similarly situated, Plaintiffs,	:	14-cv-1138
v.	:	
PAYTIME, INC., Defendant.	:	
	:	Hon. John E. Jones III
BARBARA HOLT and LINDA REDDING, individually and on behalf of all others similarly situated, Plaintiffs,	:	
v.	:	
PAYTIME HARRISBURG, INC., d/b/a PAYTIME, INC., a Pennsylvania corporation, Defendant.	:	

MEMORANDUM & ORDER

October 6, 2015

Presently pending before the Court is Plaintiffs' Motion for Leave to File First Consolidated Amended Class Action Complaint. (Doc. 49). Plaintiffs filed a

brief in support of their Motion, (Doc. 49-1), as well as a Proposed First Consolidated Amended Class Action Complaint and the original amended complaint with modifications marked. (Doc. 49, Exs. A, C).[1] Defendant did not file a formal brief in opposition but filed a letter on the Court's docket opposing the Motion on both procedural and substantive grounds. (Doc. 50).[2] For the reasons that follow, the Court shall deny this Motion.

First, contrary to Defendant's assertion, the Court does indeed have jurisdiction over motions for leave to amend a complaint following a dismissal without prejudice. *Newark Branch, N.A.A.C.P v. Town of Harrison, N.J.*, 907 F.2d 1408, 1417 (3d Cir. 1990).

The grant or denial of a motion for leave to amend is a matter committed to the sound discretion of the district court. *Id.* (citing *Foman v. Davis*, 371 U.S. 178, 182-83 (1962)). Leave to amend complaints should be "routinely granted to plaintiffs, even after judgments of dismissal have been entered against them, if the appropriate standard for leave to amend" under Federal Rule of Civil Procedure 15(a) has been met. *Id.* Rule 15(a)(2) provides that courts should "freely give leave

[1] We also note that Plaintiffs filed a Notice of Supplemental Authority on August 28, 2015. (Doc. 52).

[2] Defendant did indicate it was willing to file a "substantive response" to the Motion if the Court so desired. (Doc. 50, p. 2).

when justice so requires." FED. R. CIV. P. 15(a)(2). Courts may deny leave to amend on grounds of "undue delay, bad faith, dilatory motive, prejudice, and futility." *In re Burlington Coat Factory Securities Litigation*, 114 F.3d 1410, 1434 (3d Cir. 1997). Courts analyze "futility" under the same standard as applies to Rule 12(b)(6) motions. *Id.* In other words, a court will find amendment to be futile where the complaint, as amended, would fail to state a claim upon which relief could be granted. *Id.*

As discussed in our March 13, 2015 Memorandum and Order, (Docs. 47, 48), dismissing the instant matter for lack of standing, in order to adequately allege standing, "a plaintiff must allege personal injury fairly traceable to the defendant's allegedly unlawful conduct and likely to be redressed by the requested relief." *Allen v. Wright*, 468 U.S. 737, 751 (1984). The personal injury element of standing requires an "injury in fact," one that is "concrete in both a qualitative and temporal sense" and not merely "abstract." *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990). Further, and most importantly to our disposition of this Motion, the injury must also be actual or "imminent," not "conjectural" or "hypothetical." *Id.* In the event of a data breach, the Third Circuit has held that a plaintiff does not suffer a harm, and thus does not have standing to sue, unless plaintiff alleges actual "misuse" of the information, or that such misuse is imminent. *Reilly v. Ceridian Corp.*, 664

F.3d 38, 42 (3d Cir. 2011).

After reviewing the Consolidated Amended Class Action Complaint, ("CACAC"), we find the proposed amendments to be futile in that they fail to cure the defects in pleading which merited the Court's dismissal of the consolidated complaint in March of 2015. *See Bauchman for Bauchman v. West High School*, 132 F.3d 542, 562 (10th Cir. 1997) (affirming district court's denial of motion for leave to amend on grounds of futility because the proffered amended complaint did not cure the deficiencies in the original complaint); *Manson v. Stacescu*, 11 F.3d 1127, 1133 (2d Cir. 1993) (rejecting as futile proposed amendment of claim plaintiffs lacked standing to assert) . We still fail to see an actual or imminent injury alleged which would create standing. Despite Plaintiffs' assertion in their brief that the CACAC contains "new factual allegations" regarding the data breach, the CACAC continues to only allege that Plaintiffs and the proposed class members are at an "increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse." (Doc. 49, Ex. A, ¶ 53). Plaintiffs fail to allege facts showing why this risk of identity theft is "certainly impending" or otherwise imminent beyond references to unrelated studies and reports regarding trends in identity theft occurrence nationwide. First, mere use of the legal buzzwords of "certainly impending" or "imminent risk" does not create standing. Further, as we

stated in our March 2015 Memorandum and which we need not repeat ourselves too fulsomely today, citation to national studies is simply not enough to create standing in the matter *sub judice*. Plaintiffs themselves state in their complaint, "The only issue is when, not if, Plaintiffs and the Class will be damaged." (*Id.*, ¶ 49). Given Plaintiffs' acknowledgment that there is no injury, and that the questions remain whether and when any injuries might even occur, the Court questions why the CACAC in its current iteration was even submitted for leave to file. Indeed, as Defendant contends, the CACAC appears to be little more than an effort at a back-door, untimely motion for reconsideration.[3]

Plaintiffs cite to *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015) as very recent authority for the proposition that they have standing. In *Remijas*, the Seventh Circuit reversed the district court's dismissal of the complaint for lack of standing in a similar data breach case, finding that plaintiffs had adequately alleged imminent future injury in the form of greater susceptibility to identity theft and increased risk of fraudulent charges. The Seventh Circuit also found that the plaintiffs' expenses incurred for credit monitoring services constituted a "concrete injury" for standing purposes. *Id.* at 694. We acknowledge

[3] Plaintiffs also assert as an injury in fact in their CACAC the costs of taking precautions against identity theft such as credit monitoring services. Because we already discussed in detail this theory of standing and why it fails in our March 2015 Memorandum, (Doc. 47, p. 18), we will not replicate that exercise.

there appears to be a circuit split on the issues of whether victims of a data breach who have not yet experienced fraud or misuse of their data can adequately allege standing and whether the costs of credit monitoring can constitute an injury. However, we are bound by the Third Circuit's decision in *Reilly*, and furthermore, this Court does not necessarily agree with the reasoning in *Remijas*. *Remijas* is also somewhat distinguishable because there, the defendant, Neiman Marcus, admitted not only that their customers' personal data had been hacked and stolen, but also that 9,200 credit cards had already incurred fraudulent charges. *Id.* at 691-92.

In an attempt to adequately plead standing, Plaintiffs now also allege a claim for declaratory relief. (Doc. 49, Ex. A, ¶ 117). In order to have standing for a claim for declaratory relief, a plaintiff must show that "he has sustained or is immediately in danger of sustaining some direct injury as the result of the challenged . . . conduct and the injury or threat of injury must be both real and immediate, not conjectural or hypothetical." *Thomas v. Jones*, 428 Fed.Appx. 122, 124 (3d Cir. 2011) (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 101-02 (1983)).

Standing to seek declaratory relief is thus not significantly different, if not essentially the same, as the general standard for Article III standing. Again, we amply discussed in our March 2015 Memorandum how Plaintiffs failed to show actual or imminent injury. We have reviewed the CACAC and still fail to find an

allegation showing a threat of injury that is "both real and immediate." The Court is aware that there is indeed some possibility that some of the victims of this data breach will at some future point experience an injury in the form of identity theft or fraudulent payments. However, on the face of the complaint, it appears that no plaintiff has experienced such injury or faces an "immediate" risk of such injury. Morever, the immediacy of future injury is undermined by the fact that this data breach occurred in April 2014, a year and half ago, and yet there is still no sign of a single incident of identity theft among the Plaintiffs or proposed class.

NOW, THEREFORE, IT IS HEREBY ORDERED THAT:

1. Plaintiffs' Motion for Leave to File Consolidated Amended Class Action Complaint, (Doc. 49), is **DENIED**.

s/ John E. Jones III
John E. Jones III
United States District Judge