154 A.3d 318
Superior Court of Pennsylvania.

Barbara A. DITTMAN, Gary R. Douglas, Alice Pastirik, Joann Decolati, Tina Sorrentino, Kristen Cushman and Shannon Molyneaux, Individually and on behalf of all others similarly situated, Appellants
v.
UPMC d/b/a the University of Pittsburgh Medical Center, and UPMC McKeesport, Appellees

No. 971 WDA 2015
|
Argued May 17, 2016
|
FILED JANUARY 12, 2017
|
Reargument Denied March 20, 2017

Synopsis

Background: Employees of university medical center brought class action against medical center for negligence and breach of implied contract after a data breach, wherein the names, birth dates, social security numbers, tax information, addresses, salaries, and bank information of employees were accessed and stolen from medical center's computer systems. The Court of Common Pleas, Allegheny County, Civil Division at No(s): GD14–003285, Stanton R. Wettick, Jr., J., sustained medical center's preliminary objections, and employees appealed.

Holdings: The Superior Court, Olson, J., held that:

medical center owed no duty to its employees to prevent employees' confidential information from being stolen by third parties in a data breach, and

no consideration supported implied contract between medical center and its employees.

Affirmed.

Stabile, J., filed a concurring statement in which Olson, J., joined.

Musmanno, J., filed dissenting statement.

***320** Appeal from the Order Entered May 28, 2015, In the Court of Common Pleas of Allegheny County, Civil Division at No(s): GD14–003285, Before WETTICK, J.

Attorneys and Law Firms

Gary F. Lynch, New Castle, for appellants.

John C. Conti, Pittsburgh, for appellees.

BEFORE: OLSON, STABILE AND MUSMANNO, JJ.:

Opinion

OPINION BY OLSON, J.:

Appellants, Barbara Dittman, Gary Douglas, Alice Pastirik, Joann Decolati, Tina Sorrentino, Kristin Cushman, and Shannon Molyneaux, individually and on behalf of all others similarly situated, [1] appeal from the May 28, 2015 order sustaining preliminary objections on behalf of UPMC. After careful review, we affirm.

We summarize the relevant factual background and procedural history as follows. Appellants brought an action for negligence and breach of contract against UPMC after a data breach, wherein the ***321** names, birth dates, social security numbers, tax information, addresses, salaries, and bank information of approximately 62,000 UPMC employees and former employees were accessed and stolen from UPMC's computer systems ("the data breach"). The stolen information was used to file fraudulent tax returns and steal the tax refunds of certain employees. The digitally-stored data consisted of personal information that UPMC required employees to provide as a condition of their employment.

The exact manner in which the data breach occurred is unknown. The manner in which UPMC announced the data breach to the public and employees suggested that it was unaware of the breach, its scope, or both. In its first confirmation of the data breach in February 2014, UPMC stated that only 22 employees were affected. In March 2014, UPMC reported 322 employees' information had been stolen. In April 2014, it confirmed that information for up to 27,000 employees was compromised and at least 788 of those employees had been victims of tax

fraud. Finally, in May 2014, UPMC announced that the data breach compromised information from all of its employees.

Appellants assert that UPMC owed a legal duty to protect their personal and financial information. They also allege that UPMC failed to keep their information safe and prevent vulnerabilities in its computer system. Specifically, they allege UPMC failed to properly encrypt data, establish adequate firewalls, and implement adequate authentication protocols to protect the information in its computer network. Appellants assert that UPMC's failure to safeguard their information was the direct and proximate cause of actual damages sustained from the filing of fraudulent tax returns using their stolen information. Appellants further allege that UPMC's failure to protect their information put them at an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse in the future. This resulted in monetary damages incurred to protect themselves and their information.

Appellants brought actions for both negligence and breach of implied contract. These claims were brought on behalf of two separate but overlapping classes of similarly situated persons. The first proposed class included those current and former employees of UPMC who have already been victimized by identity theft resulting from the data breach. The second proposed class included those individuals whose personal and financial information has been stolen, and who are at an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse as a result of the data breach.

Appellants filed a class action complaint on February 27, 2014, to which UPMC filed preliminary objections on April 30, 2014. Appellants then filed the first amended class action complaint on May 16, 2014. UPMC filed renewed preliminary objections and Appellants responded by filing their second amended class action complaint on June 25, 2014. UPMC again filed preliminary objections, arguing the second amended complaint should be dismissed on the grounds that Appellants lacked standing to assert claims on behalf of individuals who had not yet been injured. UPMC further asserted that Appellants' negligence and breach of implied contract claims fail as a matter of law. Appellants responded in opposition.

The parties appeared for oral argument on UPMC's preliminary objections on October 22, 2014. The trial court then ordered both parties to file supplemental briefs on the issue of whether UPMC owed a duty to its employees with respect to the handling of their personal and financial ***322** data which UPMC requires employees produce. On May 28, 2015, the court sustained UPMC's preliminary objections and dismissed both claims. This timely appeal followed. [2]

Appellants present three issues for our review:

> 1. Does an employer have a legal duty to act reasonably in managing its computer systems to safeguard sensitive personal information collected from its employees, when the employer elects, for purposes of its own business efficiencies, to store and manage such sensitive employee data on its internet-accessible computer system, leaving it vulnerable to computer hackers, in the absence of reasonable safeguards?
>
> 2. Can a tort claim for negligence be maintained when the alleged losses, while admittedly purely economic in nature, result from the breach of a legal duty recognized by common law, and not from a duty arising under a contract?
>
> 3. Is there an implied agreement between an employer and its employees requiring the employer to act reasonably to safeguard its computer systems when the employer requires its employees, as a condition of employment, to provide sensitive personal information and then elects, for purposes of its own business efficiencies, to store and manage such sensitive employee data on its internet-accessible computer system, leaving it vulnerable to computer hackers, in the absence of such reasonable safeguarding?

Appellants' Brief at 3–4. [3]

In our review of a trial court's order sustaining preliminary objections in the form of a demurrer, we must consider all well-pleaded facts set forth in the complaint, and all inferences, in the light most favorable to the non-moving party. ***Seebold v. Prison Health Servs., Inc.***, 618 Pa. 632, 57 A.3d 1232, 1243 (2012). Our standard of review is limited to deciding whether, based on the facts and inferences, "the law says with certainty that no recovery is possible." ***Bilt–Rite Contractors, Inc. v. The Architectural Studio***, 581 Pa. 454, 866 A.2d 270, 274 (2005). We will reverse the

trial court's order sustaining preliminary objections only if there is a clear abuse of discretion or an error of law. ***Soto v. Nabisco, Inc.***, 32 A.3d 787, 790 (Pa. Super. 2011).

Appellants first argue that the trial court erred in finding that UPMC did not owe a duty of reasonable care in its collection and storage of the employees' information and data. Appellants' Brief at 21. Whether a duty exists is a question for the courts to decide. ***R.W. v. Manzek***, 585 Pa. 335, 888 A.2d 740, 746 (2005). To determine whether a duty of care exists, we look to the five factors set out in our Supreme Court's decision in ***Althaus ex. rel. Althaus v. Cohen***, 562 Pa. 547, 756 A.2d 1166, 1169 (2000) and reaffirmed in ***Seebold,*** 57 A.3d at 1243. Those factors are:

1. the relationship between the parties;

2. the social utility of the actor's conduct;

3. the nature of the risk imposed and foreseeability of the harm incurred;

4. the consequences of imposing a duty upon the actor; and,

***323** 5. the overall public interest in the proposed solution.

Althaus, 756 A.2d at 1169; ***Seebold***, 57 A.3d at 1243. None of the five factors is dispositive. ***Phillips v. Cricket Lighters***, 576 Pa. 644, 841 A.2d 1000, 1008 (2003). We will find a duty "where the balance of these factors weighs in favor of placing such a burden on a defendant." ***Id.*** at 1008–1009.

Here, the trial court found the fourth and fifth factors (consequences of imposing a duty and overall public interest in the proposed solution) were controlling and weighed in favor of not imposing a duty on UPMC. Trial Court Opinion, 2/22/2016, at 6. Additionally, the trial court concluded that there should not be a private negligence cause of action to allow recovery of economic damages against employers where confidential information is stolen by third parties in a data breach. ***Id.*** at 6, 11.

The first of the five factors in the ***Althaus*** test is the relationship between the parties. ***Althaus***, 756 A.2d at 1169. A duty is "predicated on the relationship that exists between the parties at the relevant time." ***Manzek***, 888 A.2d at 747. The relationship does not have to be specific or legally defined. ***Charlie v. Erie Ins. Exchange***, 100 A.3d 244, 252 (Pa. Super. 2014). Here, the parties had an employer-employee relationship. This type of relationship traditionally has given rise to duties on the employer. ***See e.g. Mitchell v. Scharf***, 179 Pa.Super. 220, 115 A.2d 774 (1995). Accordingly, the first factor weighs in favor of imposing a duty on UPMC to protect its employees' personal information.

The second factor looks at the social utility of the conduct at issue and is weighed against the third factor, which looks at the nature of the risk imposed and foreseeability of the harm incurred. ***Althaus***, 756 A.2d at 1169–1170. Employers, such as UPMC, have an obvious need to collect and store personal information about their employees. With the increased use of electronics and technology today, it is not surprising that this information is often stored electronically. There is an obvious social utility in this practice to promote efficiency. However, as data breaches become more common, the risk of storing information electronically increases. Also, it is foreseeable that harm from these breaches would be incurred. Our Supreme Court has, however, held that a third party committing a crime is a superseding cause. ***Ford v. Jeffries***, 474 Pa. 588, 379 A.2d 111, 115 (1977). It is well established that a defendant does not have a duty to guard against the criminal acts of superseding third-parties unless he realized, or should have realized, the likelihood of such a situation. ***Mahan v. Am–Guard, Inc.***, 841 A.2d 1052, 1060–1061 (Pa. Super. 2003) (citation omitted).

While a data breach (and its ensuing harm) is generally foreseeable, we do not believe that this possibility outweighs the social utility of electronically storing employee information. In the modern era, more and more information is stored electronically and the days of keeping documents in file cabinets are long gone. Without doubt, employees and consumers alike derive substantial benefits from efficiencies resulting from the transfer and storage of electronic data. Although breaches of electronically stored data are a potential risk, this generalized risk does not outweigh the social utility of maintaining electronically stored information. We note here that Appellants do not allege that UPMC encountered a specific threat of ***324** intrusion into its computer systems.[4] Thus, the second factor of the ***Althaus*** test, when weighed against the third factor, augurs against imposing a duty on UPMC.

The fourth factor of the *Althaus* test looks at the consequences of imposing a duty. *Althaus*, 756 A.2d at 1169. The trial court found this to be a controlling factor and found that it did not support the imposition of a duty. Trial Court Opinion, 2/22/2016, at 6. We agree. As the trial court correctly noted, "data breaches are widespread" and "there is not a safe harbor for entities storing confidential information." ***Id.*** No judicially created duty of care is needed to incentivize companies to protect their confidential information. Appellants are misguided in their assertion that the absence of a legal duty equates to the freedom of UPMC to make employees' confidential information openly available to the public. ***See*** Appellants' Brief at 33. There are still statutes and safeguards in place to prevent employers from disclosing confidential information. ***See e.g.*** 73 P.S. § 2301, *et seq.*, 74 P.S. § 201, *et seq.*, 18 U.S.C. § 2701–2712. We find it unnecessary to require employers to incur potentially significant costs to increase security measures when there is no true way to prevent data breaches altogether. Employers strive to run their businesses efficiently and they have an incentive to protect employee information and prevent these types of occurrences. As the trial court correctly found, the fourth factor weighs in favor of not imposing a duty.

Finally, the last *Althaus* factor is the public interest in imposing a duty. *Althaus*, 756 A.2d at 1169. The trial court also found this factor controlling. Trial Court Opinion, 2/22/2016, at 6. In addressing this factor, the trial court noted that creating a duty here would greatly expend judicial resources. ***Id.*** at 7. Importantly, it also considered the Pennsylvania General Assembly's legislative history on this subject and reasoned that the public interest is not served by judicial action that disrupts that deliberative process. The trial court noted:

> The General Assembly has considered and continues to consider the same issues that [Appellants] are requesting [the] court to consider under the *Seebold*/*Althaus* line of cases. The only duty that the General Assembly has chosen to impose as of today is notification of a data breach. It is not for the courts to alter the direction of the General Assembly because public policy is a matter for the [l]egislature.
>
> [The trial court finds] persuasive the [o]pinion of an Illinois appellate court in *Cooney v. Chicago Pub. Sch.*, 407 Ill.App.3d 358, 347 Ill.Dec. 733, 943 N.E.2d 23, 28–29 (2010), which rejected the plaintiffs' request that the court create a new common law duty to protect and safeguard confidential information because ***325** the [l]egislature had already imposed a duty of notification:
>
> > While we do not minimize the importance of protecting this information, we do not believe that the creation of a new legal duty beyond legislative requirements already in place is part of our role on appellate review. As noted, the legislature has specifically addressed the issue and only required the defendant to provide notice of the disclosure.

Id. at 10 (internal alterations and emphasis omitted). We agree with the trial court's reasoning and also find *Cooney* to be persuasive. The fifth factor weighs against finding a duty. Accordingly, the trial court did not err in finding that UPMC owed no duty under Pennsylvania law.

Despite finding that no duty exists, we will still examine whether the economic loss doctrine applies to the instant case. The economic loss doctrine states that "no cause of action exists for negligence that results solely in economic damages unaccompanied by physical injury or property damage." *Adams v. Copper Beach Townhome Cmty., L.P.*, 816 A.2d 301, 305 (Pa. Super. 2003). Appellants rely on *Bilt–Rite*, *supra* for the proposition that a plaintiff is not barred from recovering economic losses simply because the action sounds in tort rather than contract law. The trial court correctly noted that *Bilt–Rite* never was intended to weaken or undermine the economic loss doctrine; it was only meant to provide a narrow exception when losses are the result of reliance on the advice of professionals. ***See*** *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 177–178 (3d Cir. 2008) (holding that the economic loss doctrine barred a negligence claim resulting from a data breach). The narrow exception articulated in *Bilt–Rite* does not apply in this case. In order to recover for purely economic loss, Appellants must show that UPMC breached a duty imposed by law. ***See*** *Bilt–Rite*, 866 A.2d at 288. No such duty exists here. Without a duty imposed by law or a legally recognized special relationship, the economic loss doctrine bars Appellants claims, which assert purely economic losses. ***See*** *In re Target Corp. Data Sec. Breach Litigation*, 66 F.Supp.3d 1154, 1175–1176 (D. Minn. 2014) (noting Pennsylvania recognizes a special relationship exception to the economic loss doctrine). Accordingly, the trial court properly found that the *Althaus* factors did not weigh in favor of imposing a duty on UPMC and that the *Bilt–Rite* exception to the economic loss doctrine does not apply in the instant case.

Appellants also claim that the trial court erred when it dismissed their breach of contract claim after finding no implied contract existed between the parties. Specifically, the trial court found that UPMC did not agree to enter into an implied contract to protect Appellants' personal information. Trial Court Opinion, 2/22/2016, at 11. We agree.

An implied contract arises "where the parties agree upon the obligations to be incurred, but their intention, instead of being expressed in words, is inferred from their acts in the light of the surrounding circumstances." ***Rissi v. Capella***, 918 A.2d 131, 140 (Pa. Super. 2007), *citing* ***Martin v. Little, Brown, and Co.***, 304 Pa.Super. 424, 450 A.2d 984, 987 (1981) (emphasis omitted). Implied contracts arise under circumstances which, "according to the ordinary course of dealing and the common understanding of men, show a mutual intention to contract." ***Id.*** *citing* ***Ingrassia Const. Co., Inc. v. Walsh***, 337 Pa.Super. 58, 486 A.2d 478, 483 (1984). When ascertaining the intent of the parties, we must look to the "outward and objective manifestations" of the assent to ***326** enter into the contract. ***Ingrassia Construction Co. v. Walsh***, 337 Pa.Super. 58, 486 A.2d 478, 482–483 (1984).

Here, Appellants did not allege any objective manifestations of UPMC's intent to enter into a contract to protect their information. "A court cannot enforce a contract unless it can determine what it is." ***Ingrassia Construction Co.***, 486 A.2d at 484, *quoting* Corbin on Contracts § 95 (1963). Without any allegations that UPMC intended to enter into a contract to protect Appellants' information, the trial court did not err in dismissing the breach of contract claim.

Appellants also rely on ***McGuire v. Shubert***, 722 A.2d 1087 (Pa. Super. 1998). However, this case is distinguishable. The ***McGuire*** court implied a duty of confidentiality owed to bank customers based upon the relationship between a financial institution and its depositors. This is a relationship based in contract. ***Id.*** at 1090. This is not the same as the at-will relationship that exists between UPMC and Appellants. Thus, ***McGuire*** does not apply here.

Further, the trial court correctly determined that there was no consideration for the alleged implied contract between the parties. Trial Court Opinion, 2/22/2016, at 12–13. Consideration to establish a valid contract, either express or implied, "must be an act, a forbearance, or a return promise bargained for and given in exchange for the promise." ***Thomas v. R.J. Reynolds Tobacco Co.***, 350 Pa. 262, 38 A.2d 61, 62 (1944), *citing* Restatement (First) of Contracts § 75. "The promise must induce the detriment and the detriment must induce the promise." ***Pennsy Supply, Inc. v. Am. Ash Recycling Corp.***, 895 A.2d 595, 601 (Pa. Super. 2006) (citations omitted). Despite their contrary assertions, Appellants did not give their information to UPMC for the consideration of its safe keeping, but instead, for employment purposes. Thus, no consideration supports an implied contract between the parties in this case. Accordingly, the trial court did not err in dismissing Appellant's breach of contract claim.

Order affirmed. Application to Submit Supplemental Authority granted.

Judge Stabile files a Concurring Statement in which Judge Olson joins.

Judge Musmanno files a Dissenting Statement.

CONCURRING STATEMENT BY STABILE, J.:
I join the Majority's opinion today, but write merely to express my view that in this constantly developing area of law and technology we must proceed to establish precedent slowly and with caution. Today's decision should stand for no more than the conclusion that a legal duty was not found to exist under the facts as pled in this case. As the Majority notes, the Appellants failed to make allegations of specific threats and problems with UPMC's computer system to alter the finding of no duty in this case. ***See*** Maj. Op. at 324 n.4 (citing ***In re: The Home Depot, Inc. Customer Data Security Breach Litigation***, 2016 WL 2897520 (N.D. Ga., May 18, 2016)). Had UPMC been on notice of actual or potential security breaches of its systems, or reasonably should have anticipated that the negligent handling of confidential information would have left it vulnerable to criminal activity,[1] a different ***327** conclusion may have been reached under the factors of the ***Althaus***[2] test.

I also agree under the second factor of the ***Althaus*** test that there is significant social utility in companies like UPMC being able to store information electronically. The entire world is moving towards electronic storage of information. With this will come a greater awareness of

what is reasonable in terms of the care and storage of confidential information. At some point, the balance of weighing social utility in favor of data storage entities may shift more in favor of persons like Appellants. When harm becomes foreseeable under circumstances that commonly are understood to render storage vulnerable, the fourth ***Althaus*** factor may weigh in favor of imposing additional duties upon an actor even absent legislative action. As for the fifth and final factor under the ***Althaus*** test (the overall public interest), I believe that this factor too may shift as the foreseeability of harm changes with the evolution and increased use of this technology.

Judge Olson joins this Concurring Statement.

DISSENTING STATEMENT BY MUSMANNO, J.:
The question before this Court is whether Appellants have stated a cause of action against UPMC for negligence. More particularly, we must determine whether UPMC owed Appellants a duty of reasonable care in the collection and storage of its employees' personal information and data. After a discussion of the five factors set forth by our Supreme Court in ***Althaus ex. rel. Althaus v. Cohen***, 756 A.2d 1166 (Pa. 2000), the Majority would conclude that UPMC owed no duty to Appellants. However, upon review, I disagree with the Majority's conclusion.

"[T]o maintain a negligence action, the plaintiff must show that the defendant had a duty "to conform to a certain standard of conduct;" that the defendant breached that duty; that such breach caused the injury in question; and actual loss or damage." ***Phillips v. Cricket Lighters***, 576 Pa. 644, 841 A.2d 1000, 1008 (2003). In determining whether a duty of care exists, we consider

1. the relationship between the parties;

2. the social utility of the actor's conduct;

3. the nature of the risk imposed and foreseeability of the harm incurred;

4. the consequences of imposing a duty upon the actor; and

5. the overall public interest in the proposed solution.

Althaus, 756 A.2d at 1169; ***accord Seebold v. Prison Health Servs., Inc.***, 618 Pa. 632, 57 A.3d 1232, 1243 (2012). As the Majority correctly states, "[w]e will find a duty where the balance of these factors weigh in favor of placing such a burden on a defendant." Op. at 323 (internal quotation marks omitted) (quoting ***Phillips***, 841 A.2d at 1008–09).

The Majority would conclude that the second through fifth factors weigh against the imposition of a duty upon UMPC. Upon review, however, I would conclude that the balance of the ***Althaus*** factors weighs in favor of imposing a duty of reasonable care upon UPMC.

Regarding the first ***Althaus*** factor, the Majority correctly observes that the parties had an employer-employee relationship, and that "[t]his type of relationship traditionally has given rise to duties on the employer." Op. at 323 (citation omitted). Thus, the Majority weighed this factor in favor of imposing a duty upon UPMC. ***Id.***

328** Regarding the second and third ***Althaus factors, the Majority states that there is "an obvious social utility" in the practice of storing information electronically. ***Id.*** The Majority observes that there is an increased risk in storing electronic information, and that it is foreseeable that harm from breaches would be incurred. ***Id.*** The Majority recognizes that while the criminal acts of a third party may constituted a superseding cause,

> an actor may still be liable for his negligence[,] despite the superseding criminal acts of another if, at the time of his negligent conduct, he realized or should have realized the likelihood that such a situation might be created and that a third person might avail himself of the opportunity to commit such a tort or crime.

Op. at 323 (quoting ***Mahan v. Am–Guard, Inc.***, 841 A.2d 1052, 1061 (Pa. Super. 2003)). The Majority ultimately concludes, however, that "[w]hile a data breach (and its ensuing harm) is generally foreseeable, we do not believe that this possibility outweighs the social utility of electronically storing employee information." Op. at 323. Thus, the Majority concludes that the social utility of electronically storing information outweighs the risk of harm and the foreseeability of such harm. ***See id.*** I

believe that the Majority's conclusion is untenable, given the ubiquitous nature of electronic data storage, the risk to UPMC's employees posed by the failure to reasonably protect such information, and the foreseeability of a computer breach and subsequent identity theft.

Here, the Appellants claimed that UPMC had failed to use reasonable care in the storage of their personal information by, *inter alia*, properly encrypting the data, establishing adequate firewalls, and implementing an appropriate authentication protocol. Appellants' assertions, if proven, would establish that UPMC knew or should have realized that inadequate electronic data protections would create a likelihood that its employees' personal information would be compromised, and that a third party would avail itself of the opportunity to steal this sensitive data. ***See id.*** Under the circumstances alleged, the criminal acts of third parties do not relieve UPMC of its duty of care in the protection of Appellants sensitive personal data. Thus, I would weigh this factor in favor of imposing a duty of reasonable care upon UPMC.

I also disagree with the conclusion of the Majority that "[n]o judicially created duty of care is needed to incentivize companies to protect their confidential information." Op. at 324. The Majority would refrain from imposing a duty based upon a belief that such protection would impose significant costs upon employers to increase security measures, "when there is no true way to prevent data breaches altogether." ***Id.*** The Majority opines that "[t]here are still statutes and safeguards in place to prevent *employers* from disclosing confidential information." ***Id.*** (emphasis added).

The Majority places great weight upon the cost to UPMC of imposing a duty, and the inability to prevent every data breach. However, ***Althaus*** does not require that the proposed duty prevent *all* harm; rather, the consequences of imposing a duty of reasonable care are to be weighed. I would conclude that this factor weighs in favor of imposing a duty, when considered against the cost to employees (sometimes for years) resulting from a data breach.

Finally, I disagree with the Majority's conclusion that the public interest in imposing a duty weighs in favor of UPMC. While judicial resources may be expended during litigation of data breaches, the public has a greater interest in protecting the ***329** personal and sensitive data collected and electronically stored by employers.

Based upon the foregoing, I would reverse the Order of the trial court, and conclude that UPMC owes a duty of reasonable care to safeguard the personal information of its employees.

All Citations

154 A.3d 318, 341 Ed. Law Rep. 354, 2017 PA Super 8

Footnotes

1 Collectively, we will refer to this group as "Appellants" or "Employees."

2 Appellants filed a notice of appeal on June 22, 2015. On June 30, 2015, the trial court ordered them to file a concise statement of matters complained of on appeal ("concise statement"). ***See*** Pa.R.A.P. 1925(b). Appellants timely complied on June 21, 2015. The trial court issued its Rule 1925(a) opinion on July 22, 2015.

3 We have re-ordered the issues for ease of disposition.

4 Following oral argument, Appellants filed an Application to Submit Supplemental Authority drawing this Court's attention to a recent decision from the United States District Court for the Northern District of Georgia, ***In re: The Home Depot, Inc. Customer Data Security Breach Litigation***, 2016 WL 2897520 (N.D. Ga., May 18, 2016). In that case, the court found that Home Depot, Inc. ("Home Depot") had an independent duty to customers whose personal information was stolen from Home Depot's computers because the plaintiffs expressly pled that Home Depot knew about substantial data security risks dating back to 2008. Specifically, the court found that Home Depot had numerous warnings of a problem with its computer systems, including a hacking of the terminals in one of its Texas stores, an infection with data-stealing malware in one of its Maryland stores, and a finding by its outside security consultant that its network was vulnerable to attack and did not comply with industry standards. In the case at bar, Appellants failed to make similar allegations of specific threats and problems with UPMC's computer system.

1 As the Majority notes, citing ***Mahan v. Am–Guard, Inc.***, 841 A.2d 1052, 1060–1061 (Pa. Super. 2003).

2 ***Althaus v. Cohen***, 562 Pa. 547, 756 A.2d 1166 (2000).

End of Document